Reason T1000

Technical Manual

Distributed Multifunction Fault Recorder

Platform Hardware Version: A
Platform Software Version: 01
Publication Reference: T1000-TM-EN-2

© ALSTOM 2014. All rights reserved. Information contained in this document is indicative only. No representation or warranty is given or should be relied on that it is complete or correct or will apply to any particular project. This will depend on the technical and commercial circumstances. It is provided without liability and is subject to change without notice. Reproduction, use or disclosure to third parties, without express written authority, is strictly prohibited.

ALSTOM

Table of Contents

Configuration 7
System 8
System access 8
System Information Configuration 11
IP Configuration 12
NTP Configuration 15
Time Zone 16
System Log Configuration 18
Ports 19
Port Configuration 19
Security 23
Switch 23
Users Configuration 23
Privilege Levels Configuration 24
Authentication Method Configuration 26
SSH Configuration 27
HTTPS Configuration 28
Access Management Configuration 29
SNMP 30
SNMP System Configuration 30
SNMP Trap Configuration 31
SNMPv3 Community Configuration 34
SNMPv3 User Configuration 35
SNMPv3 Group Configuration 37
SNMPv3 View Configuration 38
SNMPv3 Access Configuration 39
RMON 40
RMON Statistics Configuration 40
RMON History Configuration 41
RMON Alarm Configuration 42
RMON Event Configuration 44
Network 45
Port Security Limit Control Configuration 45
NAS Configuration 48
ACL 55
ACL Ports Configuration 55
DHCP 57
DHCP Snooping Configuration 57
DHCP Relay Configuration 58
IP Source Guard 60
IP Source Guard Configuration 60
Static IP Source Guard Table 61
ARP Inspection 62
ARP Inspection Port Configuration 62
VLAN Mode Configuration 64
Static ARP Inspection Table 65
Dynamic ARP Inspection Table 66
AAA 68

RADIUS Server Configuration 68
TACACS+ Server Configuration 70
Aggregation *72*
Aggregation Static Configuration 72
LACP Configuration 74
Link OAM *76*
Link OAM Port Configuration 76
Link OAM Link Event Configuration 78
Loop Protection *80*
Loop Protection Configuration 80
Spanning Tree *82*
STP Bridge Configuration 82
STP MSTI Configuration 84
STP MSTI Priority Configuration 86
STP CIST Port Configuration 87
STP MSTI Port Configuration 89
IPMC Profile *90*
IPMC Profile Configurations 90
IPMC Profile Address Entry Table 92
MVR *93*
MVR Configurations 93
IPMC *96*
IGMP Snooping 96
IGMP Snooping Configuration 96
IGMP Snooping VLAN Configuration 98
IGMP Snooping Port Filtering Profile Configuration 100
MLD Snooping 101
MLD Snooping Configuration 101
MLD Snooping VLAN Configuration 103
MLD Snooping Port Filtering Profile Configuration 105
LLDP *106*
LLDP Configuration 106
LLDP Media Configuration 109
EPS *115*
EPS Configuration 115
MEP *117*
MEP Configuration 117
ERPS *119*
ERPS Configuration 119
MAC Table *121*
MAC Address Table Configuration 121
VLAN Translation *123*
Port to Group mapping Table 123
VLAN Translation Mapping Table 125
VLAN *127*
VLAN Membership Configuration 127
VLAN Port Configuration 129
Private VLAN *131*
Private VLAN Membership Configuration 131
Port Isolation Configuration 133
VCL *134*
VCL MAC-Based VLAN Configuration 134
Protocol-Based VLAN 136

Protocol to Group Mapping Table 136
Group Name to VLAN mapping Table 138
VCL IP Subnet-based VLAN Configuration 140
Ethernet Services *142*
EVC Port Configuration 142
EVC Bandwidth Profile Configuration 143
EVC Control List Configuration 145
ECE Configuration 147
QoS *151*
QoS Ingress Port Classification 151
QoS Ingress Port Policing Configuration 153
QoS Ingress Queue Policing Configuration 155
QoS Egress Port Schedulers 156
QoS Egress Port Shapers 157
QoS Egress Port Tag Remarking 158
Port DSCP Configuration 159
DSCP Translation 161
DSCP Classification 163
QoS Control List Configuration 164
Storm Control Configuration 166
QoS Weighted Random Early Detection 167
Mirroring *169*
Mirroring Configuration 169
UPnP *171*
UPnP Configuration 171
PTP *173*
PTP Clock Configuration 173
sFlow *175*
sFlow Configuration 175

Monitor 178
System *179*
System Information 179
CPU Load 181
IP Status 182
System Log Information 184
Detailed System Log Information 185
Ports *186*
Port State 186
Port Statistics Traffic Overview 187
QoS Statistics 188
QCL Status 189
Detailed Port Statistics 191
Link OAM *193*
Detailed Link OAM Port Statistics 193
Link OAM Port Configuration Status 195
Link OAM Link Event Status 197
Security *200*
Access Management Statistics 200
Network 201
Port Security 201
Port Security Switch Status 201
Port Security Port Status 203
NAS 204
NAS Switch Status 204
NAS Statistics Port 206

ACL Status 212
DHCP 214
DHCP Snooping Statistics 214
DHCP Relay Statistics 216
Dynamic ARP Inspection Table 218
Dynamic IP Source Guard Table 219
AAA 220
RADIUS Authentication Overview 220
RADIUS Authentication Statistics 222
Switch 227
RMON 227
RMON Statistics Overview 227
RMON History Overview 229
RMON Alarm Overview 231
RMON Event Overview 233
LACP 234
LACP System Status 234
LACP Port Status 235
LACP statistics 236
Loop Protection 237
Loop Protection Status 237
Spanning Tree 239
STP Bridge Status 239
STP Port Status 241
STP Port Statistics 242
MVR 243
MVR Statistics Table 243
MVR Channels Groups Information Table 245
MVR SFM Information Table 246
IPMC 248
IGMP Snooping 248
IGMP Snooping Status 248
IGMP Group Information Table 250
IGMP SFM Information Table 251
MLD Snooping 253
MLD Snooping Status 253
MLD Group Table 255
MLD SFM Information Table 256
LLDP 258
LLDP Neighbour 258
LLDP Media 260
LLDP Statistics 263
Ethernet Services 265
EVC Statistics 265
PTP 267
PTP Clock Monitor 267
MAC Table 269
Dynamic MAC Table 269
VLANs 271
VLAN Membership Status 271
VLAN Port Status 273
VCL 275
VCL MAC-Based VLAN Status 275

sFlow *276*
sFlow Statistics 276

Diagnostics 278
Ping *279*
Ping Configuration 279
Link OAM *281*
Link OAM MIB Retrieval 281
VeriPHY *282*
VeriPHY Diagnostics 282

Maintenance 284
Restart Device *285*
Maintenance Restart 285
Factory Defaults *286*
Maintenance Factory 286
Software *287*
Maintenance Software Upload 287
Image Selection 288
Configuration *289*
Running Configuration 289
Save startup-config 290
Download 291
Upload 292
Activate 293
Delete 294

1.1 Foreword

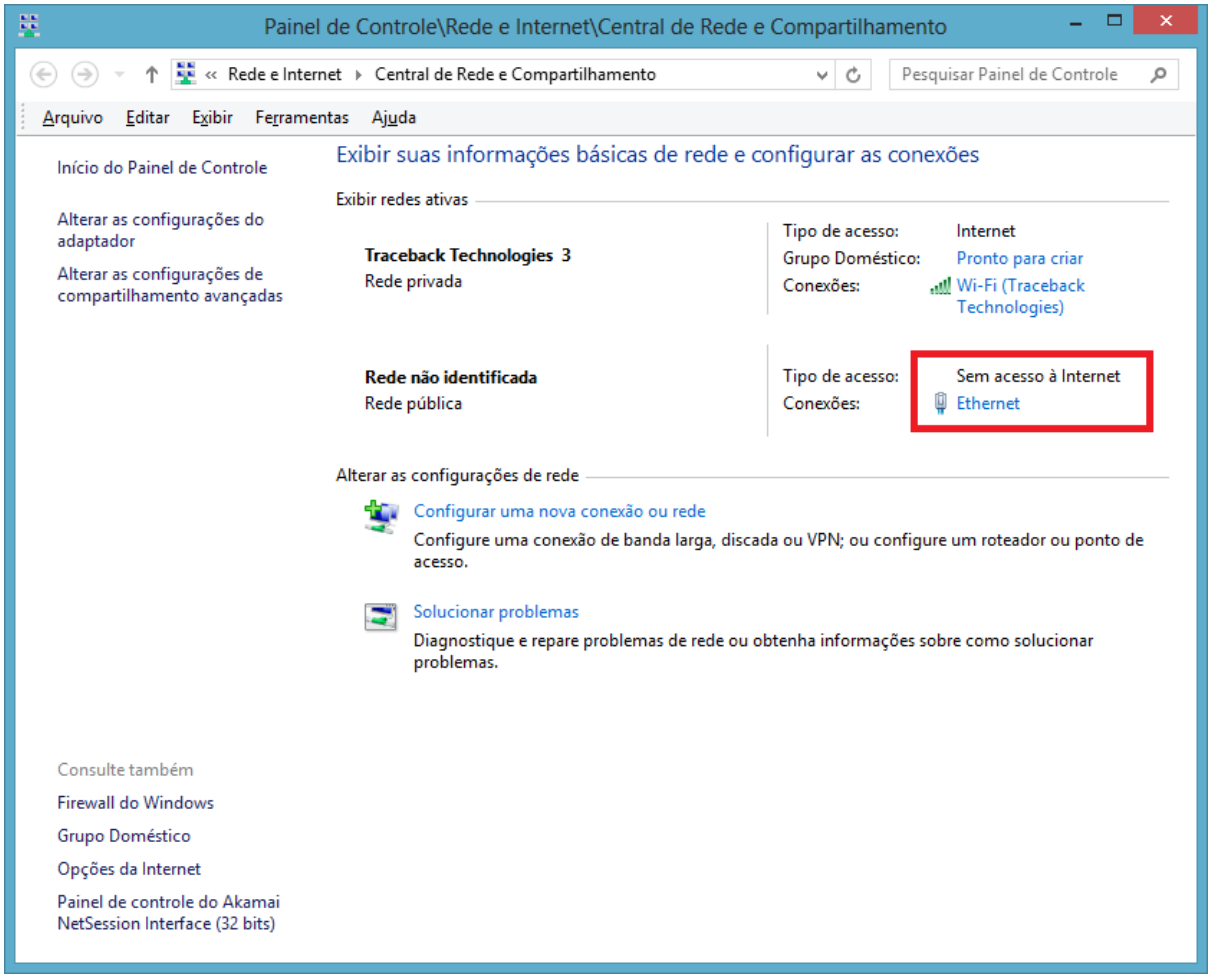
This technical manual provides a functional and technical description of Alstom Grid's RT434, as well as a comprehensive set of instructions for using the device. We have attempted to make this manual as accurate, comprehensive and user-friendly as possible. However we cannot guarantee that it is free from errors. Nor can we state that it cannot be improved. We would therefore be very pleased to hear from you if you discover any errors, or have any suggestions for improvement. All feedback should be sent to our contact centre via the following URL:

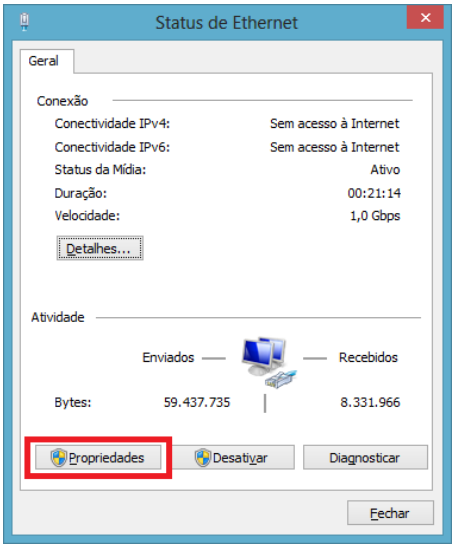
http://www.alstom.com/grid/contactcentre/

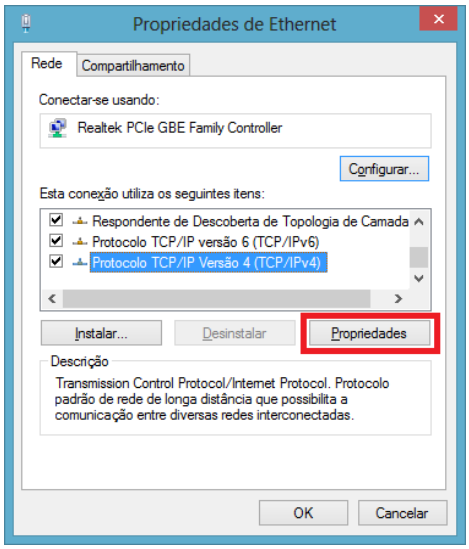
System

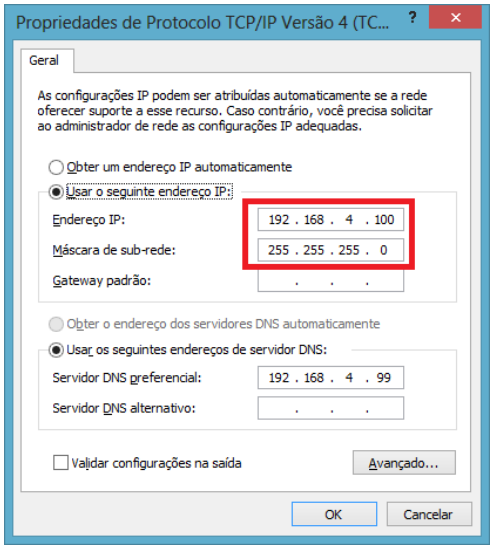
System access

To access the T1000 software configuration via web browser, configure the terminal for any address between 192.168.4.1 up to 192.168.424 and mask 2.2.2.0 for local connection. To first access, the source IP is 192.168.4.88.


Painel de Controle\Rede e Internet\Central de Rede e Compartilhamento
« Rede e Internet ▸ Central de Rede e Compartilhamento
Pesquisar Painel de Controle
Arquivo Editar Exibir Ferramentas Ajuda
Início do Painel de Controle
Alterar as configurações do adaptador
Alterar as configurações de compartilhamento avançadas
Exibir suas informações básicas de rede e configurar as conexões
Exibir redes ativas
Traceback Technologies 3
Rede privada
Tipo de acesso: Internet
Grupo Doméstico: Pronto para criar
Conexões: Wi-Fi (Traceback Technologies)
Rede não identificada
Rede pública
Tipo de acesso: Sem acesso à Internet
Conexões: Ethernet
Alterar as configurações de rede
Configurar uma nova conexão ou rede
Configure uma conexão de banda larga, discada ou VPN; ou configure um roteador ou ponto de acesso.
Solucionar problemas
Diagnostique e repare problemas de rede ou obtenha informações sobre como solucionar problemas.
Consulte também
Firewall do Windows
Grupo Doméstico
Opções da Internet
Painel de controle do Akamai NetSession Interface (32 bits)

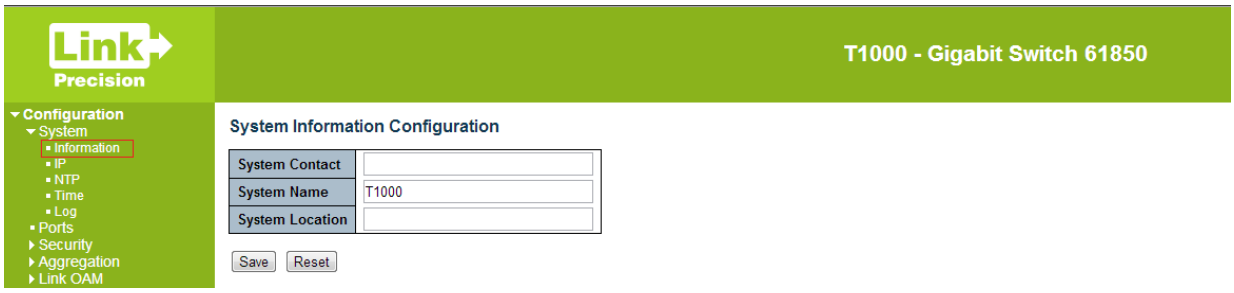

Status de Ethernet
Geral
Conexão
Conectividade IPv4: Sem acesso à Internet
Conectividade IPv6: Sem acesso à Internet
Status da Mídia: Ativo
Duração: 00:21:14
Velocidade: 1,0 Gbps
Detalhes...
Atividade
Enviados
Recebidos
Bytes: 59.437.735 8.331.966
Propriedades
Desativar
Diagnosticar
Fechar


Propriedades de Ethernet
Rede
Compartilhamento
Conectar-se usando:
Realtek PCIe GBE Family Controller
Configurar...
Esta conexão utiliza os seguintes itens:
Respondente de Descoberta de Topologia de Camada
Protocolo TCP/IP versão 6 (TCP/IPv6)
Protocolo TCP/IP Versão 4 (TCP/IPv4)
Instalar...
Desinstalar
Propriedades
Descrição
Transmission Control Protocol/Internet Protocol. Protocolo padrão de rede de longa distância que possibilita a comunicação entre diversas redes interconectadas.
OK
Cancelar


Propriedades de Protocolo TCP/IP Versão 4 (TC...
Geral
As configurações IP podem ser atribuídas automaticamente se a rede oferecer suporte a esse recurso. Caso contrário, você precisa solicitar ao administrador de rede as configurações IP adequadas.
Obter um endereço IP automaticamente
Usar o seguinte endereço IP:
Endereço IP: 192 . 168 . 4 . 100
Máscara de sub-rede: 255 . 255 . 255 . 0
Gateway padrão:
Obter o endereço dos servidores DNS automaticamente
Usar os seguintes endereços de servidor DNS:
Servidor DNS preferencial: 192 . 168 . 4 . 99
Servidor DNS alternativo:
Validar configurações na saída
Avançado...
OK
Cancelar

Use http://192.168.4.88 to first access. The default login is “admin”and have no password.

System Information Configuration



The switch system information is provided here.

System Contact

The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 2, and the allowed content is the ASCII characters from 32 to 126.

System Name

An administratively assigned name for this managed node. By convention, this is the node's fully qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 2.

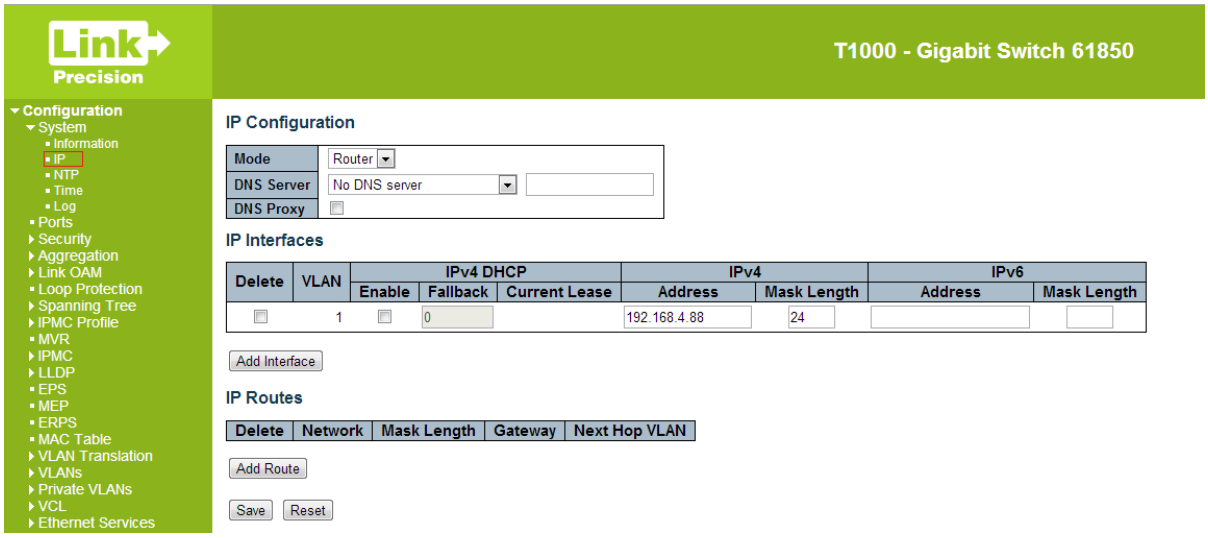
System Location

The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 2, and the allowed content is the ASCII characters from 32 to 126.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

IP Configuration



Configure IP basic settings, control IP interfaces and IP routes.
The maximum number of interfaces supported is 128 and the maximum number of routes is 32.

Basic Settings

Mode

Configure whether the IP stack should act as a Hostor a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces.

DNS Server

This setting controls the DNS name resolution done by the switch. The following modes are supported:
· From any DHCP interfaces - The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.
· No DNS server - No DNS server will be used.
· Configured - Explicitly provide the IP address of the DNS Server in dotted decimal notation.
· From this DHCP interface - Specify from which DHCP-enabled interface a provided DNS server should be preferred.

DNS Proxy

When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.

IP Interfaces

Delete

Select this option to delete an existing IP interface.

VLAN

The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating an new interface.

IPv4 DHCP Enabled

Enable the DHCP client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

IPv4 DHCP Fallback Timeout

The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 429496729 seconds.

IPv4 DHCP Current Lease

For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server.

IPv4 Address

The IPv4 address of the interface in dotted decimal notation.
If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

IPv4 Mask

The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address.
If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

IPv6 Address

The IPv6 address of the interface. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::21:cff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example: 192.1.2.34.
The field may be left blank if IPv6 operation on the interface is not desired.

IPv6 Mask

The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for a IPv6 address.
The field may be left blank if IPv6 operation on the interface is not desired.

IP Routes

Delete

Select this option to delete an existing IP route.

Network

The destination IP network or host address of this route. Valid format is dotted decimal notationor a valid IPv6 notation. A default route can use the value0.0.0.0or IPv6 :: notation.

Mask Length

The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bitsrespectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).

Gateway

The IP address of the IP gateway. Valid format is dotted decimal notationor a valid IPv6 notation. Gateway and Network must be of the same type.

Next Hop VLAN (Only for IPv6)

The VLAN ID (VID) of the specific IPv6 interface associated with the gateway.
The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.
If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway.
If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.

Buttons

ADD INTERFACE: Click to add a new IP interface. A maximum of 128 interfaces is supported.
ADD ROUTE: Click to add a new IP route. A maximum of 32routes is supported.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

NTP Configuration

Configure NTP on this page.

Mode

Indicates the NTP mode operation. Possible modes are:
Enabled: Enable NTP client mode operation.
Disabled: Disable NTP clinet mode operation.

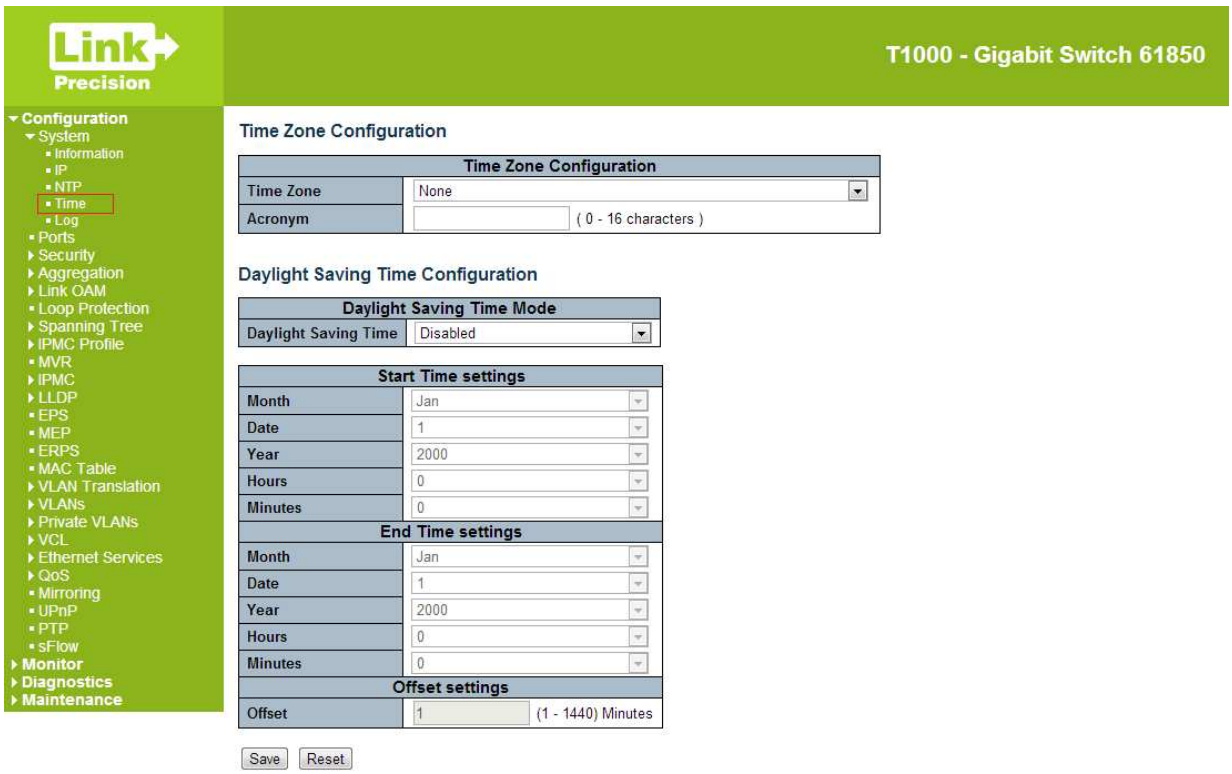
Server

Provide the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::21:cff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

Time Zone



This page allows you to configure the Time Zone.

Time Zone Configuration

· Time Zone - Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click SAVE to set.
· Acronym - User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range: Up to 16 characters)

Daylight Saving Time Configuration

This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default: Disabled)

Recurring Configurations

Start time settings

· Week - Select the starting week number.
· Day - Select the starting day.
· Month - Select the starting month.
· Hours - Select the starting hour.
· Minutes - Select the starting minute.

End time settings

· Week - Select the ending week number.
· Day - Select the ending day.
· Month - Select the ending month.

· Hours - Select the ending hour.
· Minutes - Select the ending minute.

Offset settings
· Offset - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

Non Recurring Configurations

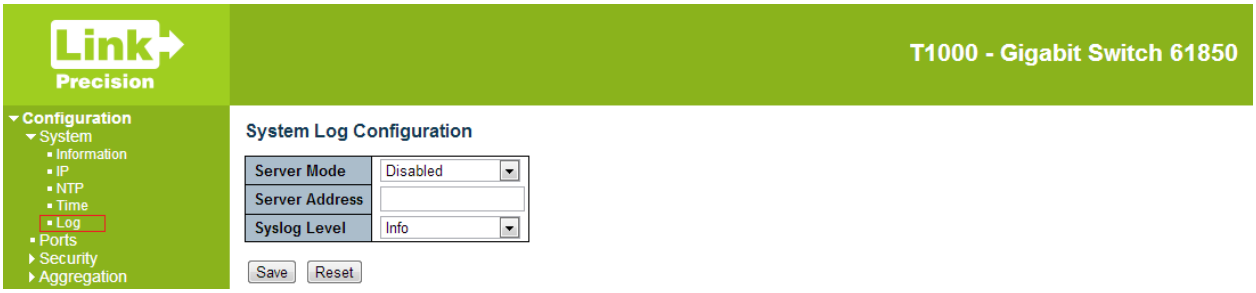
Start time settings
· Month - Select the starting month.
· Date - Select the starting date.
· Year - Select the starting year.
· Hours - Select the starting hour.
· Minutes - Select the starting minute.

End time settings
· Month - Select the ending month.
· Date - Select the ending date.
· Year - Select the ending year.
· Hours - Select the ending hour.
· Minutes - Select the ending minute.

Offset settings
· Offset - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

Buttons
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

System Log Configuration



Configure System Log on this page.

Server Mode

Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 14 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are:

· Enabled: Enable server mode operation.
· Disabled: Disable server mode operation.

Server Address

Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.

Syslog Level

Indicates what kind of message will send to syslog server. Possible modes are:
Info: Send informations, warnings and errors.
Warning: Send warnings and errors.
Error: Send errors.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

Ports

Port Configuration

This page displays current port configurations. Ports can also be configured here.

Port

This is the logical port number for this row.

Link

The current link state is displayed graphically. Green indicates the link is up and red that it is down.

Current Link Speed

Provides the current link speed of the port.

Configured Link Speed

Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are:
Disabled - Disables the switch port operation.
Auto - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.
10Mbps HDX - Forces the cu port in 10Mbps half duplex mode.
10Mbps FDX - Forces the cu port in 10Mbps full duplex mode.
100Mbps HDX - Forces the cu port in 100Mbps half duplex mode.

100Mbps FDX - Forces the cu port in 100Mbps full duplex mode.
1Gbps FDX - Forces the port in 1Gbps full duplex
2.Gbps FDX - Forces the Serdes port in 2.Gbps full duplex mode.

SFP_Auto_AMS - Automatically determines the speed of the SFP. Note: There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode. Cu port is set in Auto mode.
100-FX - SFP port in 100-FX speed. Cu port disabled.
100-FX_AMS - Port in AMS mode. SFP port in 100-FX speed. Cu port in Auto mode.
1000-X - SFP port in 1000-X speed. Cu port disabled.
1000-X_AMS - Port in AMS mode. SFP port in 1000-X speed. Cu port in Auto mode.
Ports in AMS mode with 1000-X speed has Cu port preferred.
Ports in AMS mode with 1000-X speed has fiber port preferred.
Ports in AMS mode with 100-FX speed has fiber port preferred.

Flow Control

When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner.
When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.
Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.

Maximum Frame Size

Enter the maximum frame size allowed for the switch port, including FCS.

Excessive Collision Mode

Configure port transmit collision behavior.
Discard: Discard frame after 16 collisions (default).
Restart: Restart backoff algorithm after 16 collisions.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.
REFRESH: Click to refresh the page. Any changes made locally will be undone.

EMC tests were performed according to IEC 602-26 referring to the following standards

IEC 61000-4-2:2008	6kV contact / 8KV air
IEC 61000-4-3:2006	10 V/m
IEC 61000-4-4:2012	2 KV @ KHz
IEC 61000-4-:200	Differential mode: 1KV Common mode: 2KV
IEC 61000-4-6:2008	10V
IEC 61000-4-8:2009	30A/m continuos - 300A/m @ 1s.
IEC 61000-4-11:2004 IEC 61000-4-29:2000	A.C. and d.c. voltage dips Test level: 0% residual voltage Duration time a.c.: 1 cycle d.c.: 16,6ms Test level: 40% residual voltage Duration time a.c.: 12 cycles d.c.: 200ms Test level: 70% residual voltage Duration time a.c.: 30 cycles d.c.:00ms A.C. and d.c. voltage interruptions Test level: 0% residual voltage Duration time a.c.: 300 cycles d.c.: s
IEC 61000-4-17:1999	Test level: 1 % of rated d.c. value Test frequency: 120Hz, sinusoidal waveform.
IEC 61000-4-18:2006	Voltage oscillation frequency: 1MHz Differential mode: 1kV peak voltage; Common mode 2,kV peak voltage

Gradual Startup	Shut-down ramp: 60s Power off: m Start-up ramp: 60s
CISPR11:2009	Radiated emission 30 to 230MHz - 0dB(µV/m) quasi peak at 3m 230 to 1000MHz - 7dB(µV/m) quasi peak at 3m
CISPR22:2008	Radiated emission Limits: 1 to 2GHz - 6dB(µV/m) average; 76dB(µV/m) peak at 3m Limits defined by considering the maximum internal frequency of 12MHz Conducted emission Limits: 0.1 to 0.0MHZ - 79dB(µV) quasi peak; 66dB(µV) average 0. to 30MHz - 73dB(µV) quasi peak; 60dB(µV) average

Safety	IEC 602-27

Environment	
IEC 60068-2-1	-40°C, 16 hours (Cold)
IEC 60068-2-2	+8°C, 16 hours (Dry heat)
IEC 60068-2-30	9% no condensation, °C (Damp heat)
IEC 60068-2-14	-40°C to 8ºC / 9 hours / 2 cycles (Change of temperature)
IEC 602-21-1	Class 2 (Vibration)
IEC 602-21-2	Class 1 (Shock)

Security

Switch

Users Configuration

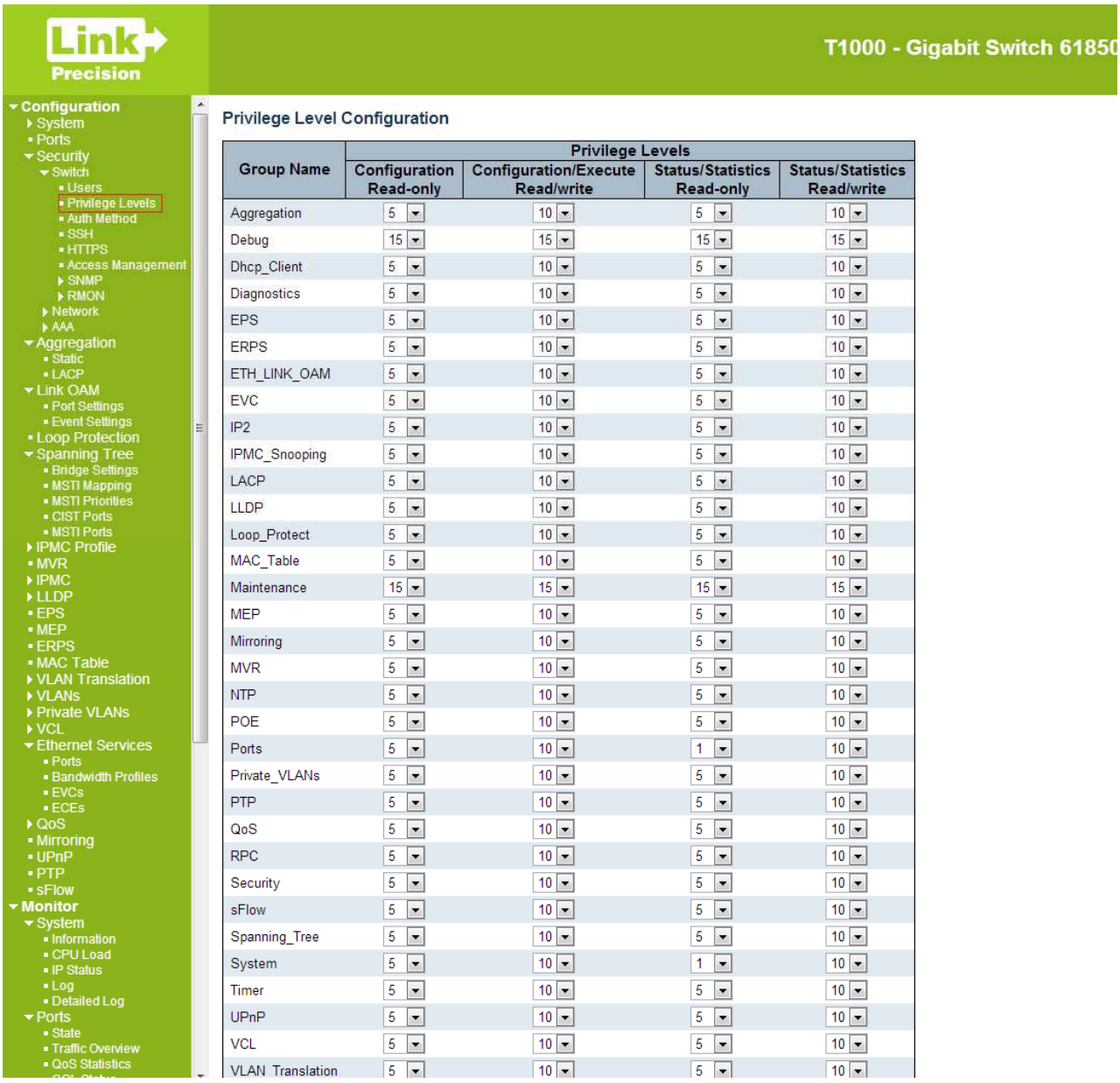
This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.
The displayed values for each user are:

User Name
The name identifying the user. This is also a link to Add/Edit User.

Privilege Level
The privilege level of the user. The allowed range is 1 to1. If the privilege level value is 1, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 1. Generally, the privilege level 1 can be used for an administrator account, privilege level 10 for a standard user account and privilege level for a guest account.

Buttons
ADD NEW USER: Click to add a new user.

Privilege Levels Configuration



This page provides an overview of the privilege levels.

Group Name

The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:
System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.
Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.
IP: Everything except 'ping'.
Port: Everything except 'VeriPHY'.
Diagnostics: 'ping' and 'VeriPHY'.
Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.
Debug: Only present in CLI.

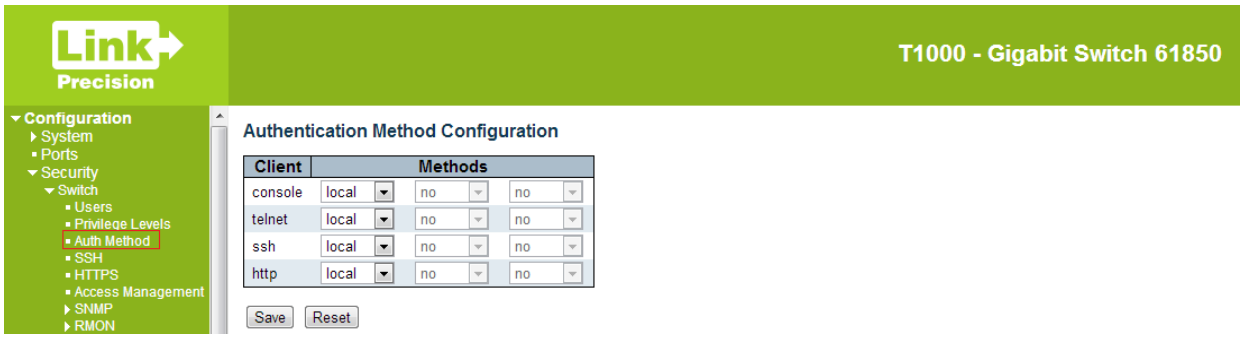
Privilege Levels

Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

Authentication Method Configuration



This page allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.
The table has one row for each client type and a number of columns, which are:

Client

The management client for which the configuration below applies.

Methods

Method can be set to one of the following values:

- no: Authentication is disabled and login is not possible.
- local: Use the local user database on the switch for authentication.
- radius: Use remote RADIUS server(s) for authentication.
- tacacs+: Use remote TACACS+ server(s) for authentication.

Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

SSH Configuration

Configure SSH on this page.

Mode

Indicates the SSH mode operation. Possible modes are:
Enabled: Enable SSH mode operation.
Disabled: Disable SSH mode operation.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

HTTPS Configuration

Configure HTTPS on this page.

Mode

Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are:
Enabled: Enable HTTPS mode operation.
Disabled: Disable HTTPS mode operation.

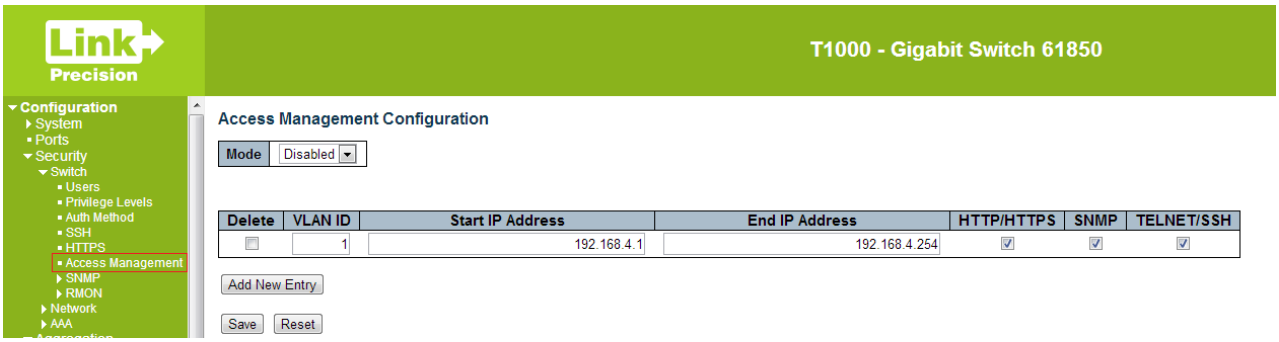
Automatic Redirect

Indicates the HTTPS redirect mode operation. It only significant if HTTPS mode "Enabled" is selected. Automatically redirects web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled. Possible modes are:
Enabled: Enable HTTPS redirect mode operation.
Disabled: Disable HTTPS redirect mode operation.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

Access Management Configuration



Configure access management table on this page. The maximum number of entries is 16. If the application's type match any one of the access management entries, it will allow access to the switch.

Mode

Indicates the access management mode operation. Possible modes are:
Enabled: Enable access management mode operation.
Disabled: Disable access management mode operation.

Delete

Check to delete the entry. It will be deleted during the next save.

VLAN ID

Indicates the VLAN ID for the access management entry.

Start IP address

Indicates the start IP address for the access management entry.

End IP address

Indicates the end IP address for the access management entry.

HTTP/HTTPS

Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

SNMP

Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

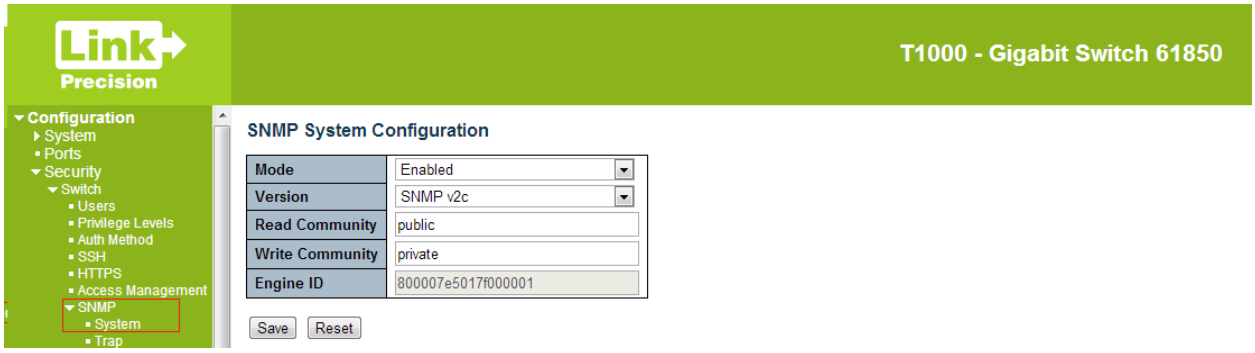
TELNET/SSH

Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Buttons

ADD NEW ENTRY: Click to add a new access management entry.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

SNMP



SNMP System Configuration

Configure SNMP on this page.

Mode

Indicates the SNMP mode operation. Possible modes are:
Enabled: Enable SNMP mode operation.
Disabled: Disable SNMP mode operation.

Version

Indicates the SNMP supported version. Possible versions are:
SNMP v1: Set SNMP supported version 1.
SNMP v2c: Set SNMP supported version 2c.
SNMP v3: Set SNMP supported version 3.

Read Community

Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 2, and the allowed content is the ASCII characters from 33 to 126.
The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Write Community

Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 2, and the allowed content is the ASCII characters from 33 to 126.
The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Engine ID

Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

SNMP Trap Configuration

Configure SNMP trap on this page.

Trap Mode

Indicates the SNMP trap mode operation. Possible modes are:
Enabled: Enable SNMP trap mode operation.
Disabled: Disable SNMP trap mode operation.

Trap Version

Indicates the SNMP trap supported version. Possible versions are:
SNMP v1: Set SNMP trap supported version 1.
SNMP v2c: Set SNMP trap supported version 2c.
SNMP v3: Set SNMP trap supported version 3.

Trap Community

Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 2, and the allowed content is ASCII characters from 33 to 126.

Trap Destination Address

Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').
And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

Trap Destination IPv6 Address

Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::21:cff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Trap Authentication Failure

Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are:
Enabled: Enable SNMP trap authentication failure.

Disabled: Disable SNMP trap authentication failure.

Trap Link-up and Link-down
Indicates the SNMP trap link-up and link-down mode operation. Possible modes are:
Enabled: Enable SNMP trap link-up and link-down mode operation.
Disabled: Disable SNMP trap link-up and link-down mode operation.

Trap Inform Mode
Indicates the SNMP trap inform mode operation. Possible modes are:
Enabled: Enable SNMP trap inform mode operation.
Disabled: Disable SNMP trap inform mode operation.

Trap Inform Timeout (seconds)
Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.

Trap Inform Retry Times
Indicates the SNMP trap inform retry times. The allowed range is 0 to 2.

Trap Probe Security Engine ID
Indicates the SNMP trap probe security engine ID mode of operation. Possible values are:
Enabled: Enable SNMP trap probe security engine ID mode of operation.
Disabled: Disable SNMP trap probe security engine ID mode of operation.

Trap Security Engine ID
Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

Trap Security Name
Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Buttons
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

Trap Destination Configurations
Configure trap destinations on this page.

Name
Indicates the trap Configuration's name. Indicates the trap destination's name.

Enable
Indicates the trap destination mode operation. Possible modes are:
Enabled: Enable SNMP trap mode operation.
Disabled: Disable SNMP trap mode operation.

Version
Indicates the SNMP trap supported version. Possible versions are:
SNMPv1: Set SNMP trap supported version 1.
SNMPv2c: Set SNMP trap supported version 2c.
SNMPv3: Set SNMP trap supported version 3.

Trap Community

Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 2, and the allowed content is ASCII characters from 33 to 126.

Destination Address

Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').
And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.
Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::21:cff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

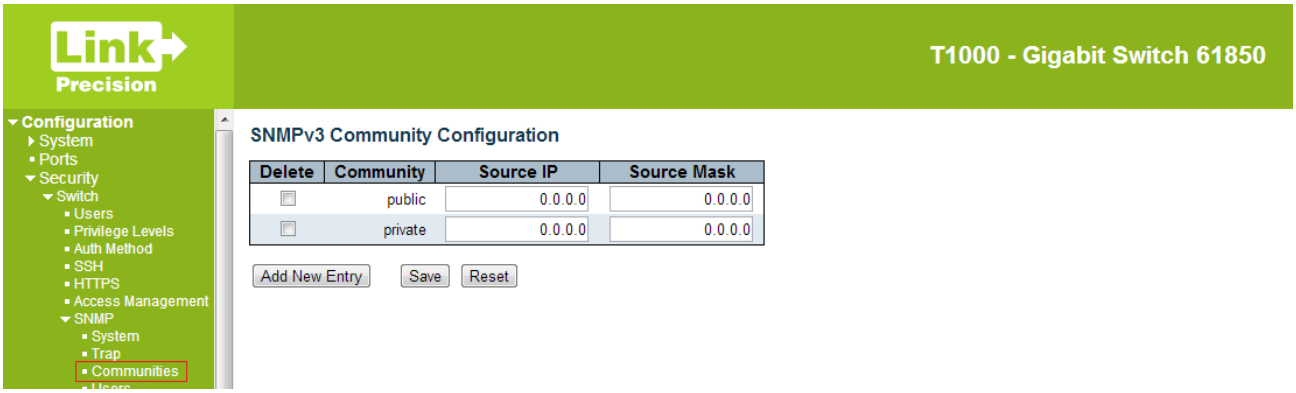
Destination port

Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~63.

Buttons

ADD NEW ENTRY: Click to add a new user.

SNMPv3 Community Configuration



Configure SNMPv3 community table on this page. The entry index key is Community.

Delete

Check to delete the entry. It will be deleted during the next save.

Community

Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.

Source IP

Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.

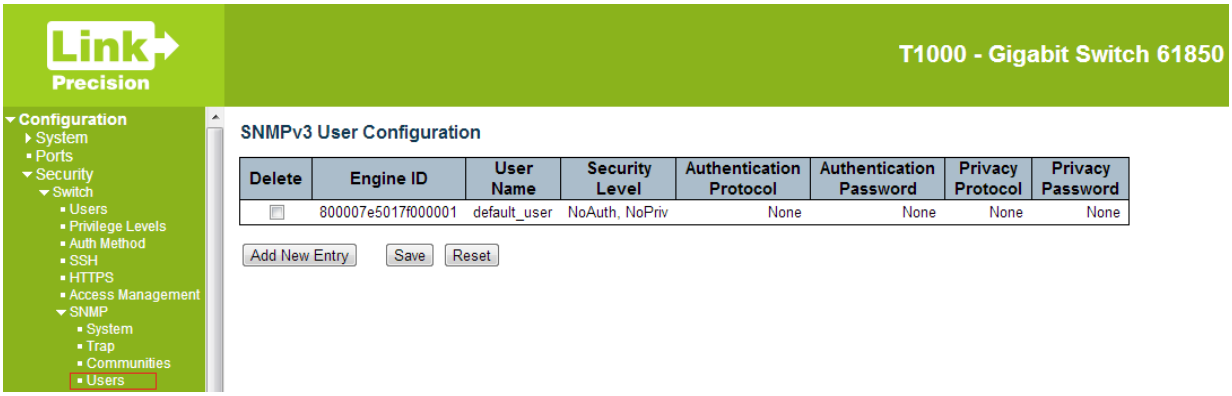
Source Mask

Indicates the SNMP access source address mask.

Buttons

ADD NEW ENTRY: Click to add a new community entry.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

SNMPv3 User Configuration



Configure SNMPv3 user table on this page. The entry index keys are Engine ID and User Name.

Delete

Check to delete the entry. It will be deleted during the next save.

Engine ID

An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.

User Name

A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level

Indicates the security model that this entry should belong to. Possible security models are:
NoAuth, NoPriv: No authentication and no privacy.
Auth, NoPriv: Authentication and no privacy.
Auth, Priv: Authentication and privacy.
The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Protocol

Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:
None: No authentication protocol.
MD: An optional flag to indicate that this user uses MD authentication protocol.
SHA: An optional flag to indicate that this user uses SHA authentication protocol.
The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

Authentication Password

A string identifying the authentication password phrase. For MD authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

Privacy Protocol

Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:
None: No privacy protocol.
DES: An optional flag to indicate that this user uses DES authentication protocol.
AES: An optional flag to indicate that this user uses AES authentication protocol.

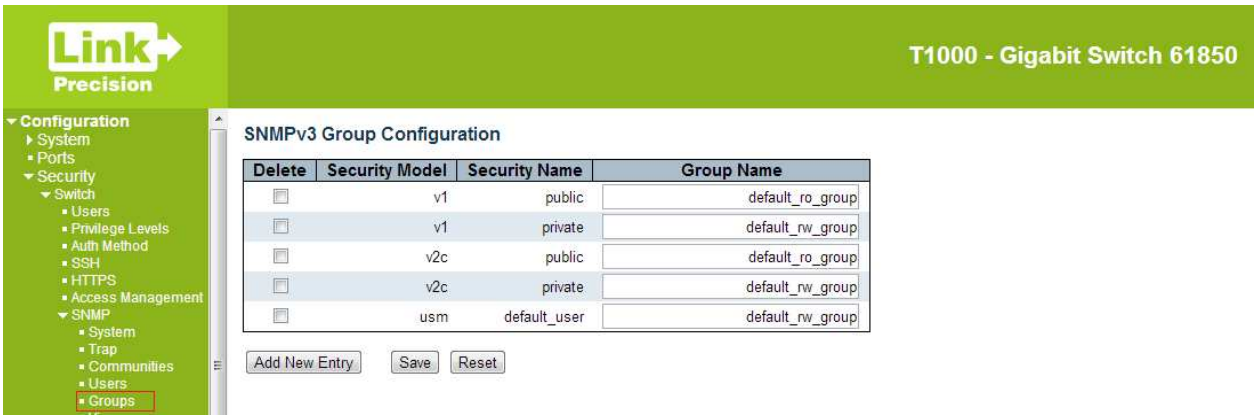
Privacy Password

A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

ADD NEW ENTRY: Click to add a new user entry.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

SNMPv3 Group Configuration



Configure SNMPv3 group table on this page. The entry index keys are Security Model and Security Name.

Delete

Check to delete the entry. It will be deleted during the next save.

Security Model

Indicates the security model that this entry should belong to. Possible security models are:
v1: Reserved for SNMPv1.
v2c: Reserved for SNMPv2c.
usm: User-based Security Model (USM).

Security Name

A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

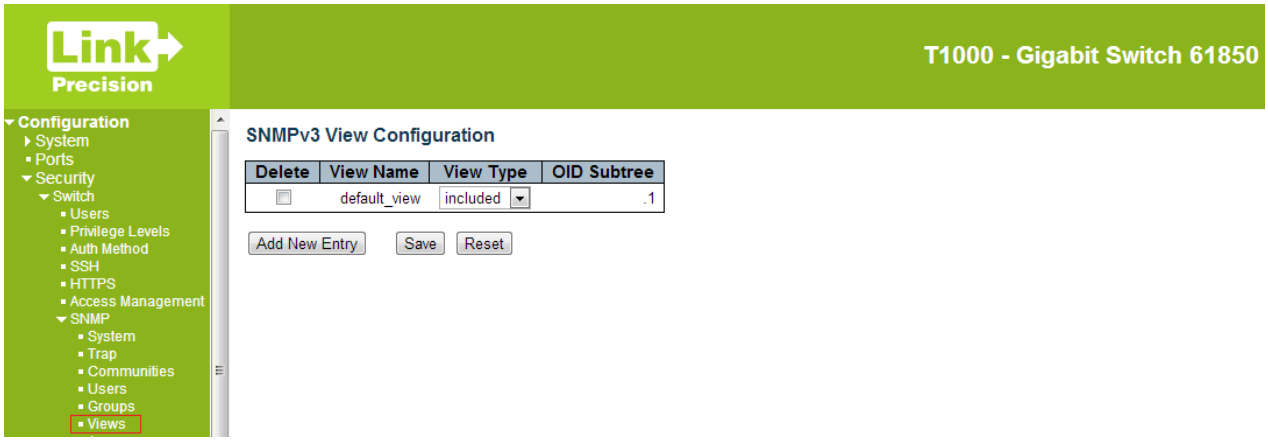
Group Name

A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

ADD NEW ENTRY: Click to add a new user entry.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

SNMPv3 View Configuration



Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.

Delete

Check to delete the entry. It will be deleted during the next save.

View Name

A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

View Type

Indicates the view type that this entry should belong to. Possible view types are:
included: An optional flag to indicate that this view subtree should be included.
excluded: An optional flag to indicate that this view subtree should be excluded.
In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.

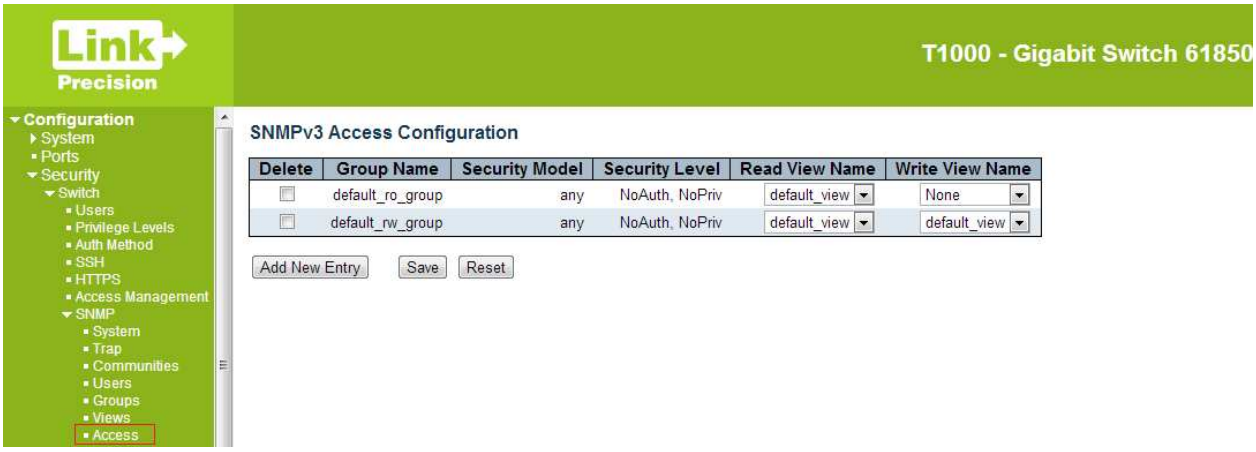
OID Subtree

The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Buttons

ADD NEW ENTRY: Click to add a new user entry.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

SNMPv3 Access Configuration



Configure SNMPv3 access table on this page. The entry index keys are Group Name, Security Model andSecurity Level.

Delete

Check to delete the entry. It will be deleted during the next save.

Group Name

A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Model

Indicates the security model that this entry should belong to. Possible security models are:
any: Any security model accepted(v1|v2c|usm).
v1: Reserved for SNMPv1.
v2c: Reserved for SNMPv2c.
usm: User-based Security Model (USM).

Security Level

Indicates the security model that this entry should belong to. Possible security models are:
NoAuth, NoPriv: No authentication and no privacy.
Auth, NoPriv: Authentication and no privacy.
Auth, Priv: Authentication and privacy.

Read View Name

The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Write View Name

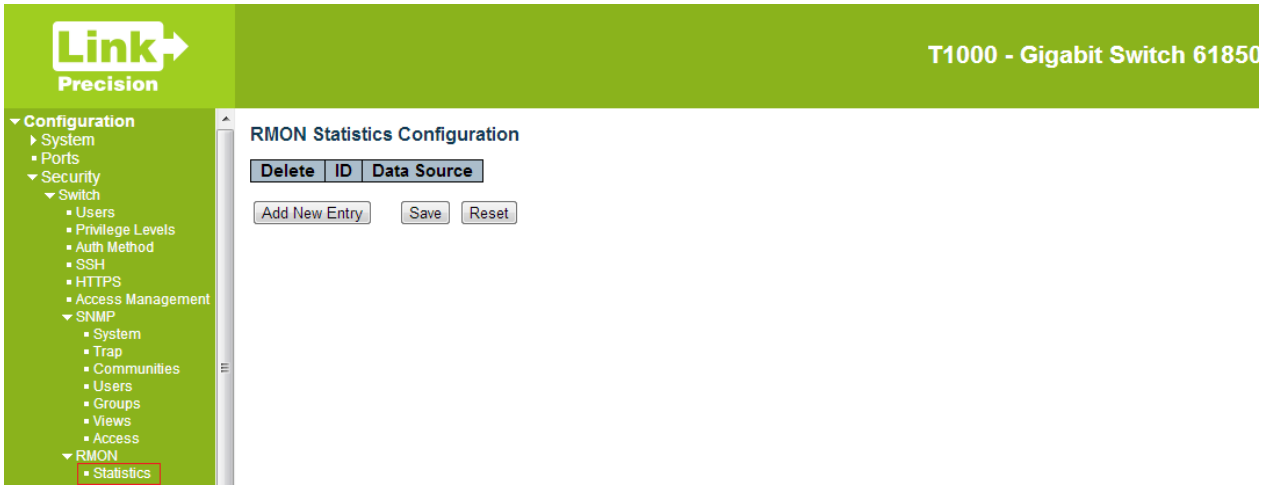
The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

ADD NEW ENTRY: Click to add a new user entry.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

RMON

RMON Statistics Configuration



Configure RMON Statistics table on this page. The entry index key is ID.

Delete

Check to delete the entry. It will be deleted during the next save.

ID

Indicates the index of the entry. The range is from 1 to 63.

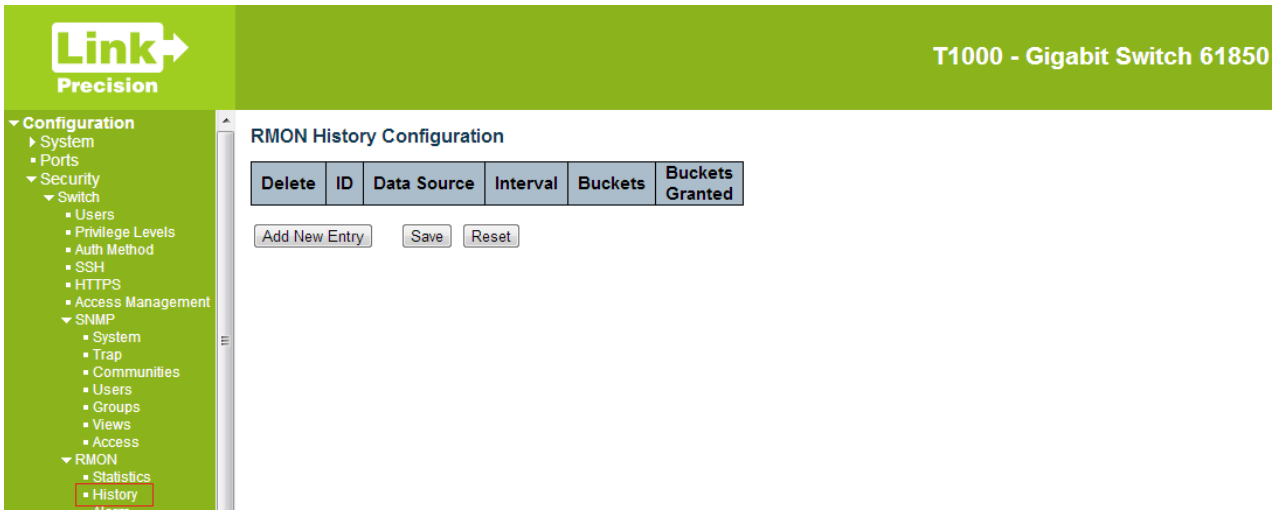
Data Source

Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port , the value is 200

Buttons

ADD NEW ENTRY: Click to add a new user entry.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

RMON History Configuration



Configure RMON History table on this page. The entry index key is ID.

Delete

Check to delete the entry. It will be deleted during the next save.

ID

Indicates the index of the entry. The range is from 1 to 63.

Data Source

Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port , the value is 200.

Interval

Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.

Buckets

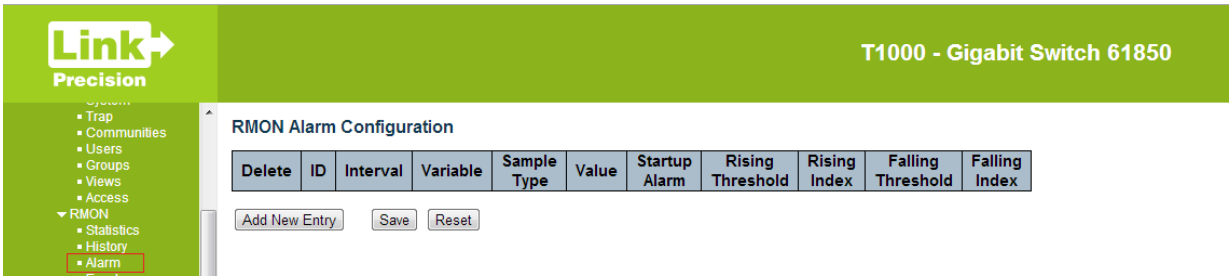
Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 0.

Buckets Granted

The number of data shall be saved in the RMON.

Buttons

ADD NEW ENTRY: Click to add a new user entry.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.



RMON Alarm Configuration

Configure RMON Alarm table on this page. The entry index key is ID.

Delete

Check to delete the entry. It will be deleted during the next save.

ID

Indicates the index of the entry. The range is from 1 to 63.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.

Variable

Indicates the particular variable to be sampled, the possible variables are:
InOctets: The total number of octets received on the interface, including framing characters.
InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol.
InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.
InDiscards: The number of inbound packets that are discarded even the packets are normal.
InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol.
OutOctets: The number of octets transmitted out of the interface , including framing characters.
OutUcastPkts: The number of uni-cast packets that request to transmit.
OutNUcastPkts: The number of broad-cast and multi-cast packets that request to transmit.
OutDiscards: The number of outbound packets that are discarded event the packets is normal.
OutErrors: The The number of outbound packets that could not be transmitted because of errors.
OutQLen: The length of the output packet queue (in packets).

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:
Absolute: Get the sample directly.
Delta: Calculate the difference between samples (default).

Value

The value of the statistic during the last sampling period.

Startup Alarm

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:
RisingTrigger alarm when the first value is larger than the rising threshold.
FallingTrigger alarm when the first value is less than the falling threshold.
RisingOrFallingTrigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

Rising Threshold

Rising threshold value (-2147483648-2147483647).

Rising Index

Rising event index (1-63).

Falling Threshold

Falling threshold value (-2147483648-2147483647)

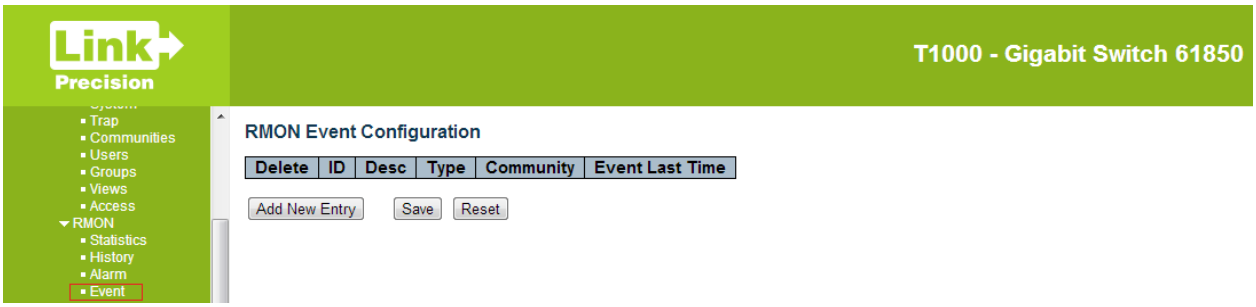
Falling Index

Falling event index (1-63).

Buttons

ADD NEW ENTRY: Click to add a new user entry.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

RMON Event Configuration



Configure RMON Event table on this page. The entry index key is ID.

Delete

Check to delete the entry. It will be deleted during the next save.

ID

Indicates the index of the entry. The range is from 1 to 63.

Desc

Indicates this event, the string length is from 0 to 127, default is a null string.

Type

Indicates the notification of the event, the possible types are:
none: The total number of octets received on the interface, including framing characters.
log The number of uni-cast packets delivered to a higher-layer protocol.
snmptrap: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.
logandtrap: The number of inbound packets that are discarded even the packets are normal.

Community

Specify the community when trap is sent, the string length is from 0 to 127, default is "public".

Event Last Time

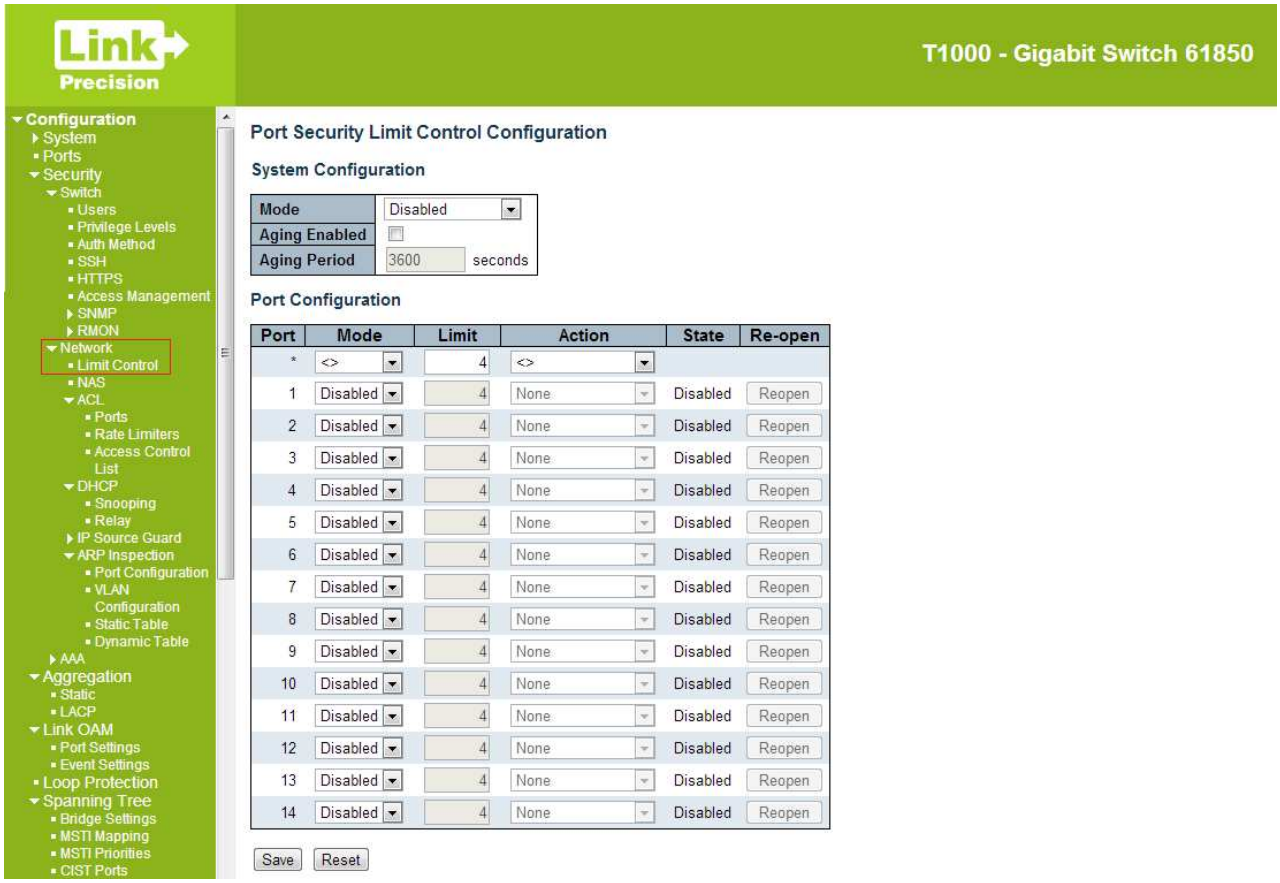
Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

ADD NEW ENTRY: Click to add a new user entry.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

Network

Port Security Limit Control Configuration



This page allows you to configure the Port Security Limit Control system and port settings.

Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.
The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learnt on the port.
The Limit Control configuration consists of two sections, a system- and a port-wide.

System Configuration

Mode

Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled

If checked, secured MAC addresses are subject to aging as discussed under Aging Period .

Aging Period

If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.
The Aging Period can be set to a number between 10 and 10,000,000 seconds.
To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration

The table has one row for each port on the switch and a number of columns, which are:

Port

The port number to which the configuration below applies.

Mode

Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

Limit

The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.
The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Action

If Limit is reached, the switch can take one of the following actions:
None: Do not allow more than Limit MAC addresses on the port, but take no further action.
Trap: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.
Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:
1) Boot the switch,
2) Disable and re-enable Limit Control on the port or theswitch,
3) Click the Reopen button.
Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

State

This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:
Disabled: Limit Control is either globally disabled or disabled on the port.
Ready: The limit is not yet reached. This can be shown for all actions.
Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set toNone or Trap.
Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Actionis set to Shutdown or Trap & Shutdown.

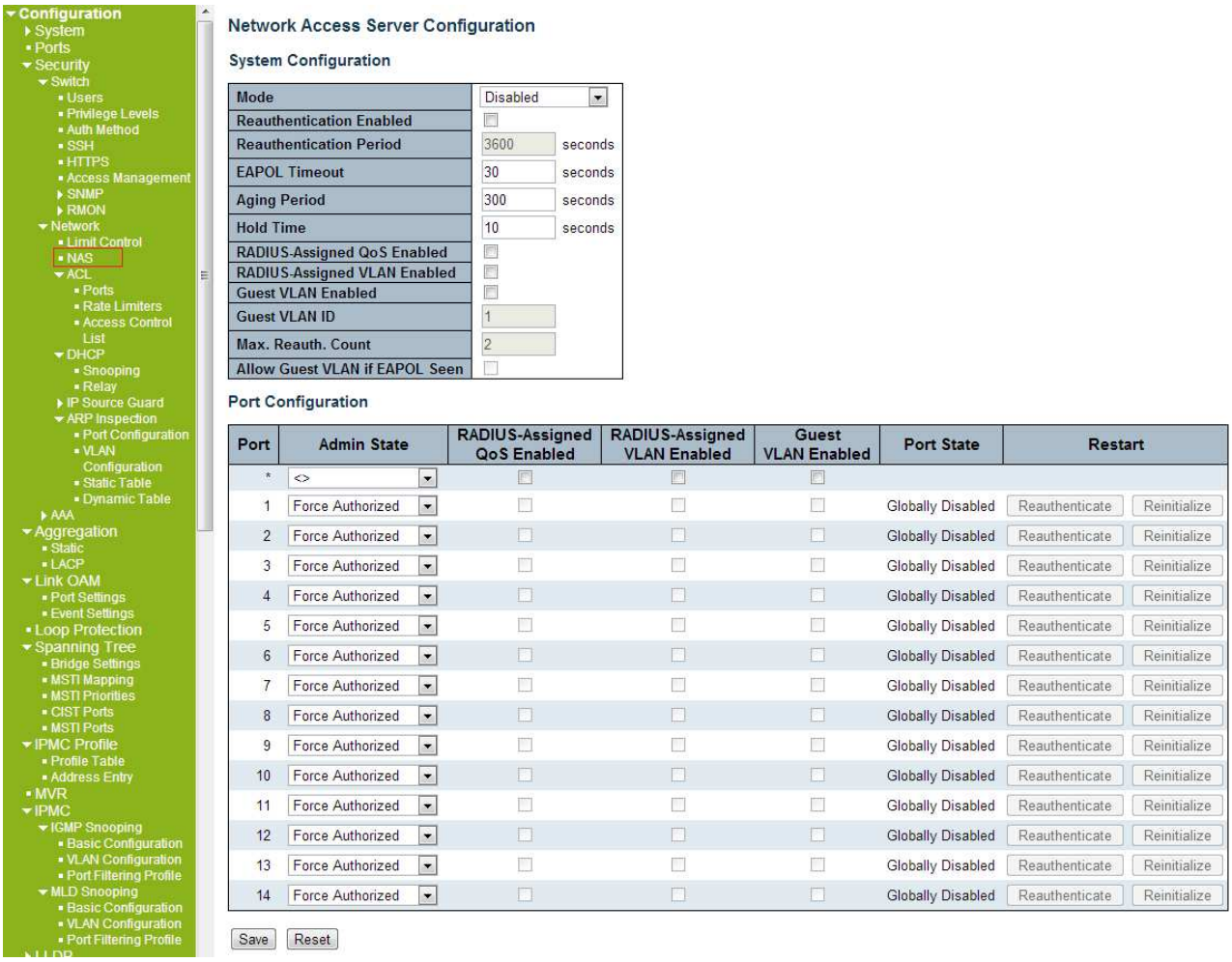
Re-open Button

If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Actionsection.
Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.

Buttons

REFRESH: Click to refresh the page. Note that non-committed changes will be lost.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

NAS Configuration



This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.
The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Configuration→Security→AAA" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.
MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.
The NAS configuration consists of two sections, a system- and a port-wide.

System Configuration

Mode

Indicates if NAS is globally enabled or disabled on theswitch. If globally disabled, all ports are allowed forwarding of frames.

Reauthentication Enabled

If checked, successfully authenticated supplicants/clientsare reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.
For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

Reauthentication Period

Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.

EAPOL Timeout

Determines the time for retransmission of Request Identity EAPOL frames.
Valid values are in the range 1 to 63 seconds. This has no effect for MAC-based ports.

Aging Period

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:
· Single 802.1X
· Multi 802.1X
· MAC-Based Auth.
When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.
If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.
For ports in MAC-based Auth. mode, reauthenticationdoesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

Hold Time

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:
· Single 802.1X
· Multi 802.1X
· MAC-Based Auth.
If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.
In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.
The Hold Time can be set to a number between 10 and 1000000 seconds.

RADIUS-Assigned QoS Enabled

RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description).

The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

RADIUS-Assigned VLAN Enabled

RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (seeRADIUS-Assigned VLAN Enabled below for a detailed description).

The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

Guest VLAN Enabled

A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.
The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

Guest VLAN ID

This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled.
Valid values are in the range [1; 409].

Max. Reauth. Count

The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option isglobally enabled.
Valid values are in the range [1; 2].

Allow Guest VLAN if EAPOL Seen

The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port.
The value can only be changed if the Guest VLAN option isglobally enabled.

Port Configuration

The table has one row for each port on the switch and a number of columns, which are:

Port

The port number for which the configuration below applies.

Admin State

If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:

Force Authorized
In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

Force Unauthorized
In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

Port-based 802.1X
In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUSpackets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.
When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.
Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Single 802.1X
In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.
Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X
Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics.In Multi 802.1X, one or more supplicants can get authenticated on the same port at the

same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.
In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.
The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Controlfunctionality.

MAC-based Auth.
Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD-Challenge authentication method, so the RADIUS server must be configured accordingly.
When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.
The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

RADIUS-Assigned QoS Enabled

When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e.
• Port-based 802.1X
• Single 802.1X

RADIUS attributes used in identifying a QoS Class:
The User-Priority-Table attribute defined in RFC467forms the basis for identifying the QoS Class in an Access-Accept packet.
Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:
• All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

RADIUS-Assigned VLAN Enabled

When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the

RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.
If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).
This option is only available for single-client modes, i.e.
• Port-based 802.1X
• Single 802.1X
For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

RADIUS attributes used in identifying a VLAN ID:
RFC2868 and RFC380 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:
· The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.
· The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):
  - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).
  - Value of Tunnel-Type must be set to "VLAN" (ordinal 13).
  - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 409].

Guest VLAN Enabled

When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.
This option is only available for EAPOL-based modes, i.e.:
· Port-based 802.1X
· Single 802.1X
· Multi 802.1X
For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

Guest VLAN Operation:
When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.
Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

Port State

The current state of the port. It can undertake one of the following values:
Globally Disabled: NAS is globally disabled.
Link Down: NAS is globally enabled, but there is no link on the port.
Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.
Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.
X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

Restart

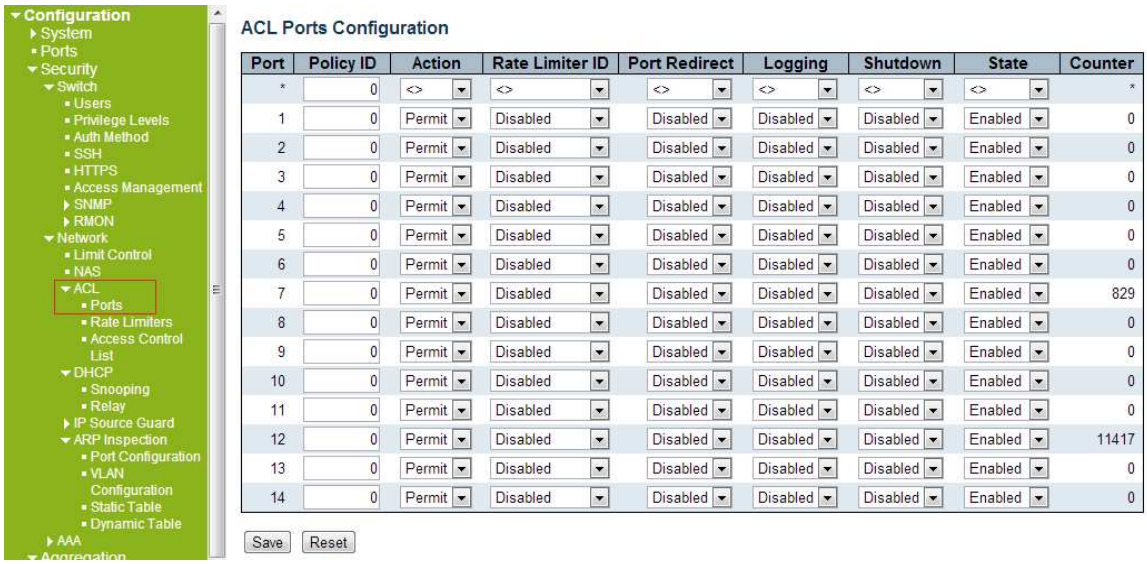
Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-basedmode.
Clicking these buttons will not cause settings changed on the page to take effect.
Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.
Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

Buttons

REFRESH: Click to refresh the page. Note that non-committed changes will be lost.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

ACL

ACL Ports Configuration



Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

Port

The logical port for the settings contained in the same row.

Policy ID

Select the policy to apply to this port. The allowed values are0 through 2. The default value is 0.

Action

Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

Rate Limiter ID

Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".

Port Redirect

Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".

Logging

Specify the logging operation of this port. The allowed values are:
Enabled: Frames received on the port are stored in the System Log.
Disabled: Frames received on the port are not logged.
The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.

Shutdown

Specify the port shut down operation of this port. The allowed values are:

Enabled: If a frame is received on the port, the port will be disabled.
Disabled: Port shut down is disabled.
The default value is "Disabled".

State

Specify the port state of this port. The allowed values are:
Enabled: To reopen ports by changing the volatile port configuration of the ACL user module.
Disabled: To close ports by changing the volatile port configuration of the ACL user module.
The default value is "Enabled".

Counter

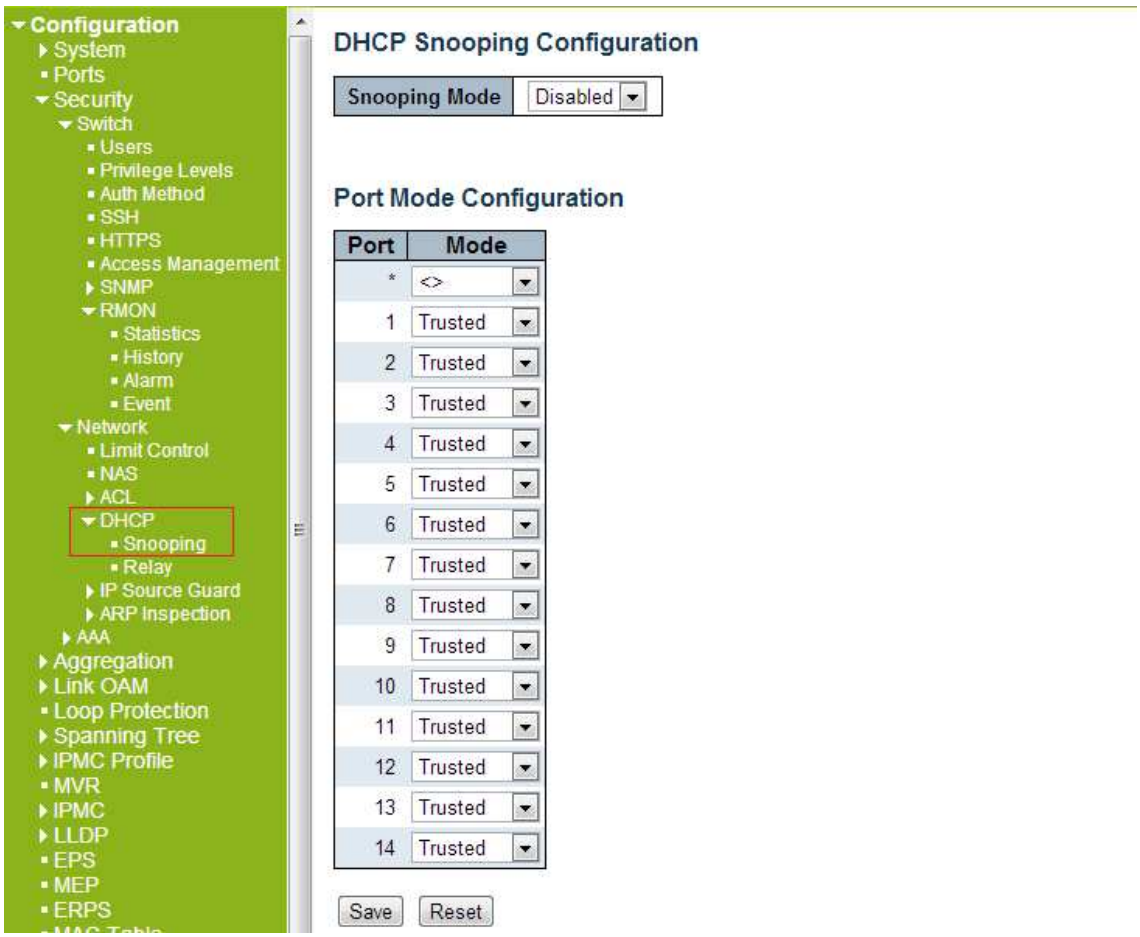
Counts the number of frames that match this ACE.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.
REFRESH: Click to refresh the page; any changes made locally will be undone.
CLEAR: Click to clear the counters.

DHCP

DHCP Snooping Configuration



Configure DHCP Snooping on this page.

Snooping Mode

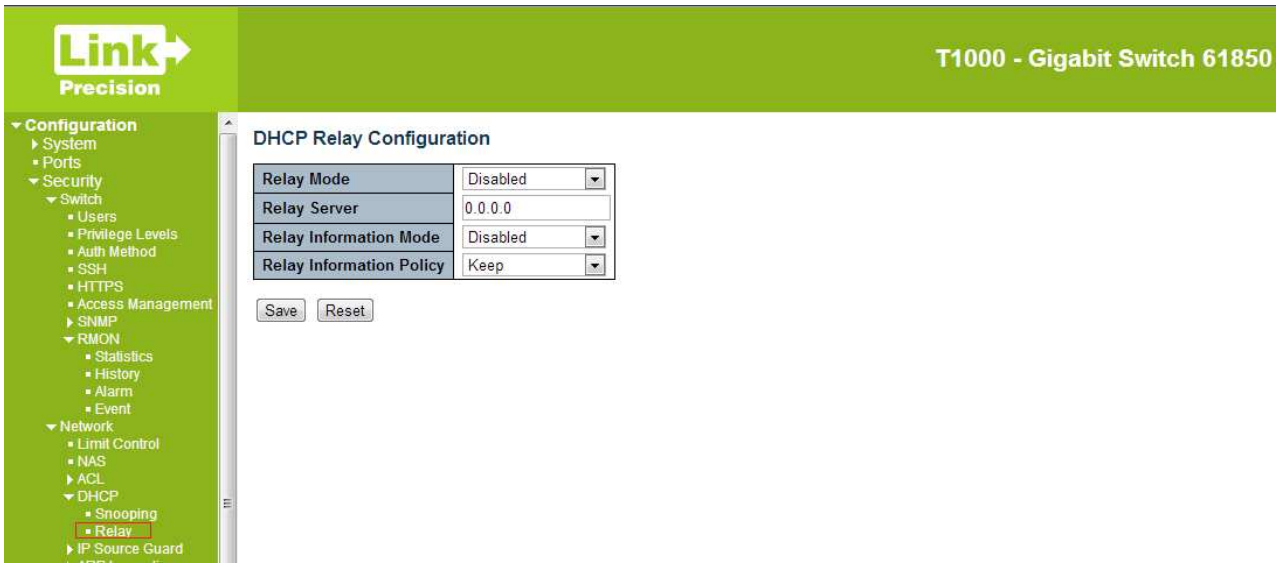
Indicates the DHCP snooping mode operation. Possible modes are:
Enabled: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.
Disabled: Disable DHCP snooping mode operation.

Port Mode Configuration

Indicates the DHCP snooping port mode. Possible port modes are:
Trusted: Configures the port as trusted source of the DHCP messages.
Untrusted: Configures the port as untrusted source of the DHCP messages.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.



DHCP Relay Configuration

Configure DHCP Relay on this page.

Relay Mode

Indicates the DHCP relay mode operation.
Possible modes are:
Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.
Disabled: Disable DHCP relay mode operation.

Relay Server

Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain.

Relay Information Mode

Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.
Possible modes are:
Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.
Disabled: Disable DHCP relay information mode operation.

Relay Information Policy

Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will

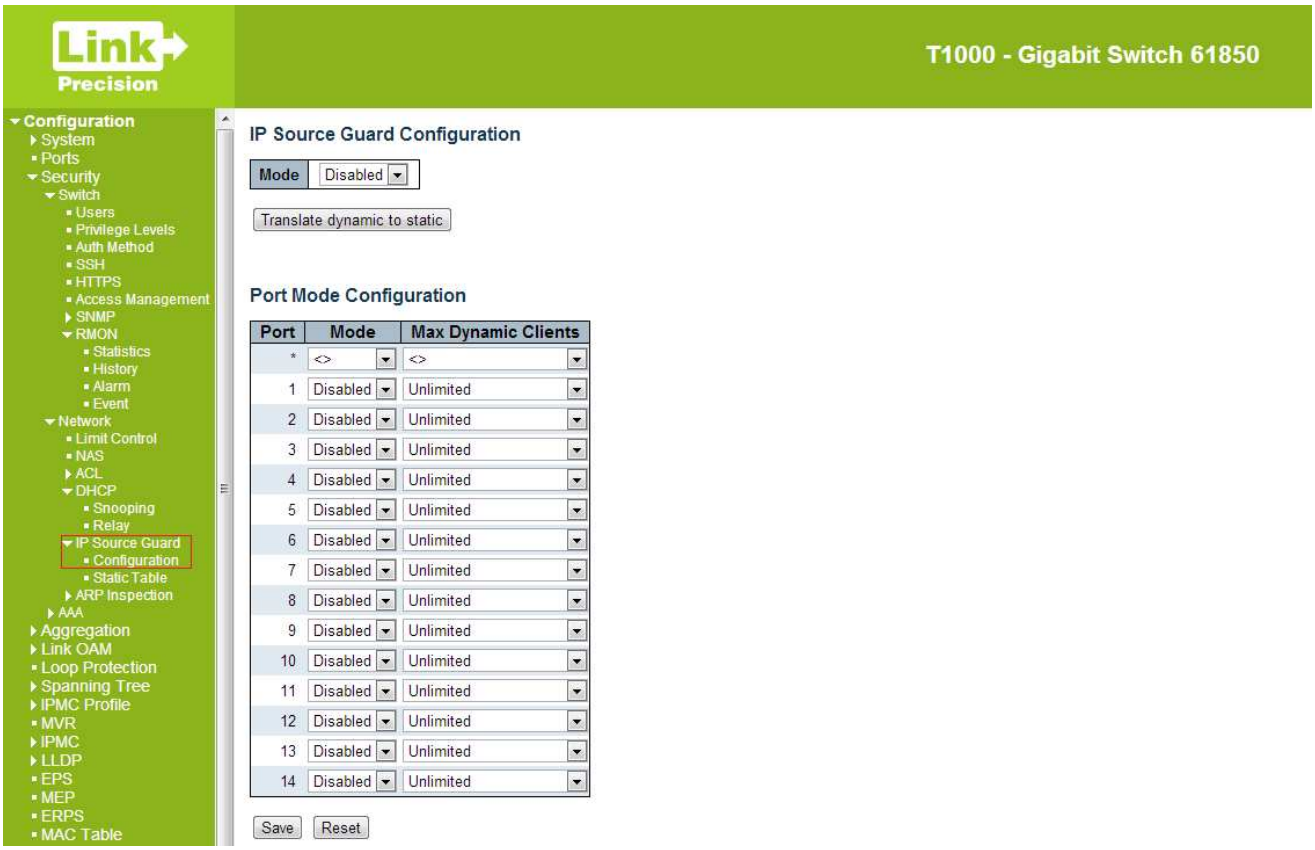
enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:
Replace: Replace the original relay information when a DHCP message that already contains it is received.
Keep: Keep the original relay information when a DHCP message that already contains it is received.
Drop: Drop the package when a DHCP message that already contains relay information is received.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

IP Source Guard

IP Source Guard Configuration



This page provides IP Source Guard related configuration.

Mode of IP Source Guard Configuration

Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration

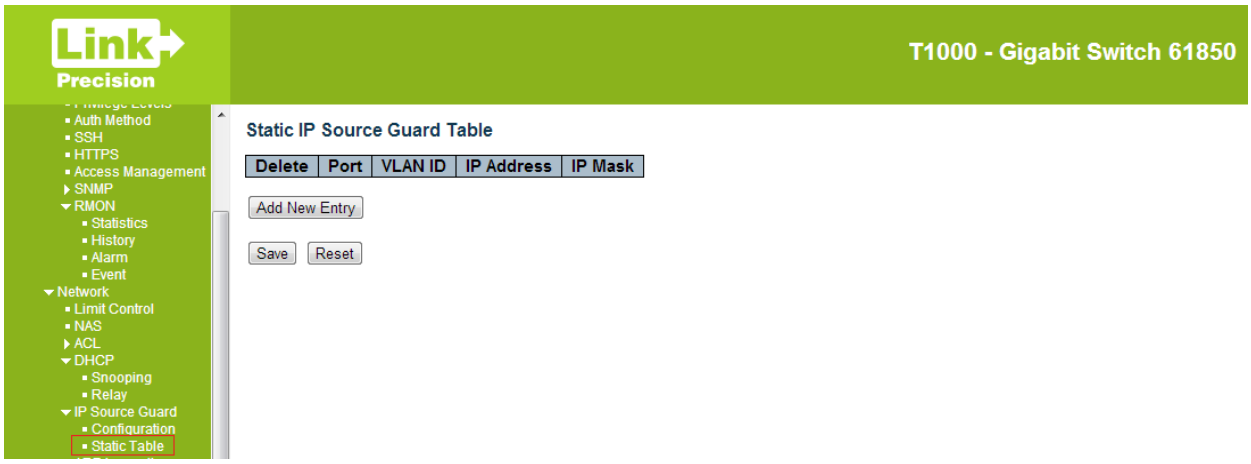
Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

Max Dynamic Clients

Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.
TRANSLATE DYNAMIC TO STATIC: Click to translate all dynamic entries to static entries.



Static IP Source Guard Table

Delete

Check to delete the entry. It will be deleted during the next save.

Port

The logical port for the settings.

VLAN ID

The vlan id for the settings.

IP Address

Allowed Source IP address.

IP Mask

It can be used for calculating the allowed network with IP address.

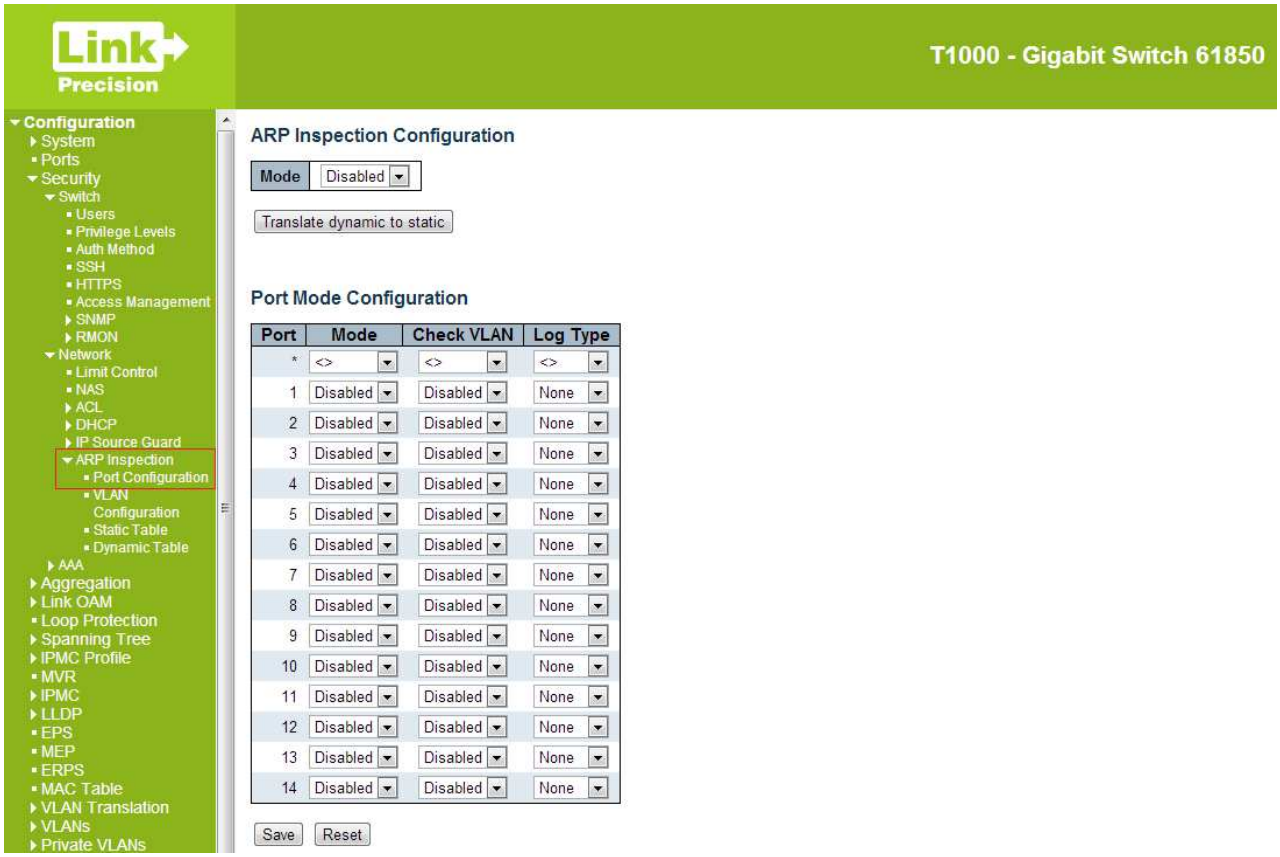
Buttons

ADD NEW ENTRY: Click to add a new entry to the Static IP Source Guard table.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

ARP Inspection

ARP Inspection Port Configuration

This page provides ARP Inspection related configuration.



Mode of ARP Inspection Configuration

Enable the Global ARP Inspection or disable the Global ARP Inspection.

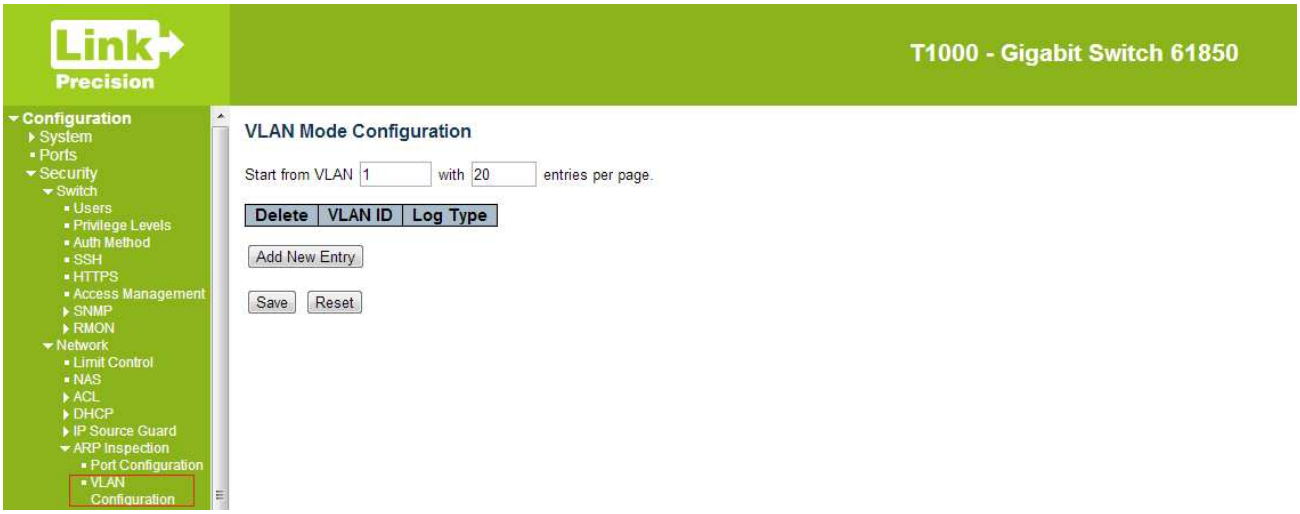
Port Mode Configuration

Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:
Enabled: Enable ARP Inspection operation.
Disabled: Disable ARP Inspection operation.
If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are:
Enabled: Enable check VLAN operation.
Disabled: Disable check VLAN operation.
Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are:
None: Log nothing.
Deny: Log denied entries.
Permit: Log permitted entries.
ALL: Log all entries.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.
TRANSLATE DYNAMIC TO STATIC: Click to translate all dynamic entries to static entries.

VLAN Mode Configuration



This page provides VLAN mode related configuration.

Navigating the VLAN Configuration

Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the closest next VLAN Table match. The will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the button to start over.

VLAN Mode Configuration

Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting.

Possible types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons

ADD NEW ENTRY: Click to add a new VLAN to the ARP Inspection VLAN table.

SAVE: Click to save changes.

RESET: Click to undo any changes made locally and revert to previously saved values.

Static ARP Inspection Table

Delete

Check to delete the entry. It will be deleted during the next save.

Port

The logical port for the settings.

VLAN ID

The vlan id for the settings.

MAC Address

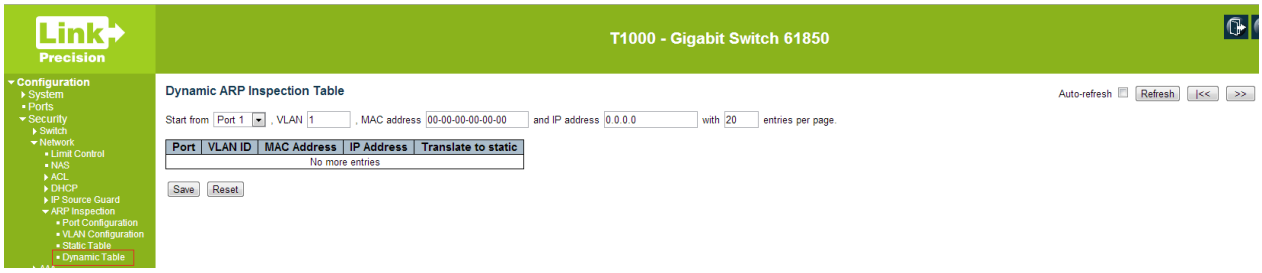
Allowed Source MAC address in ARP request packets.

IP Address

Allowed Source IP address in ARP request packets.

Buttons

ADD NEW ENTRY: Click to add a new VLAN to the ARP Inspection VLAN table.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.



Dynamic ARP Inspection Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.
The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.
The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

ARP Inspection Table Columns

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the ARP traffic is permitted.

MAC Address

User MAC address of the entry.

IP Address

User IP address of the entry.

Translate to static

Select the checkbox to translate the entry to static entry.

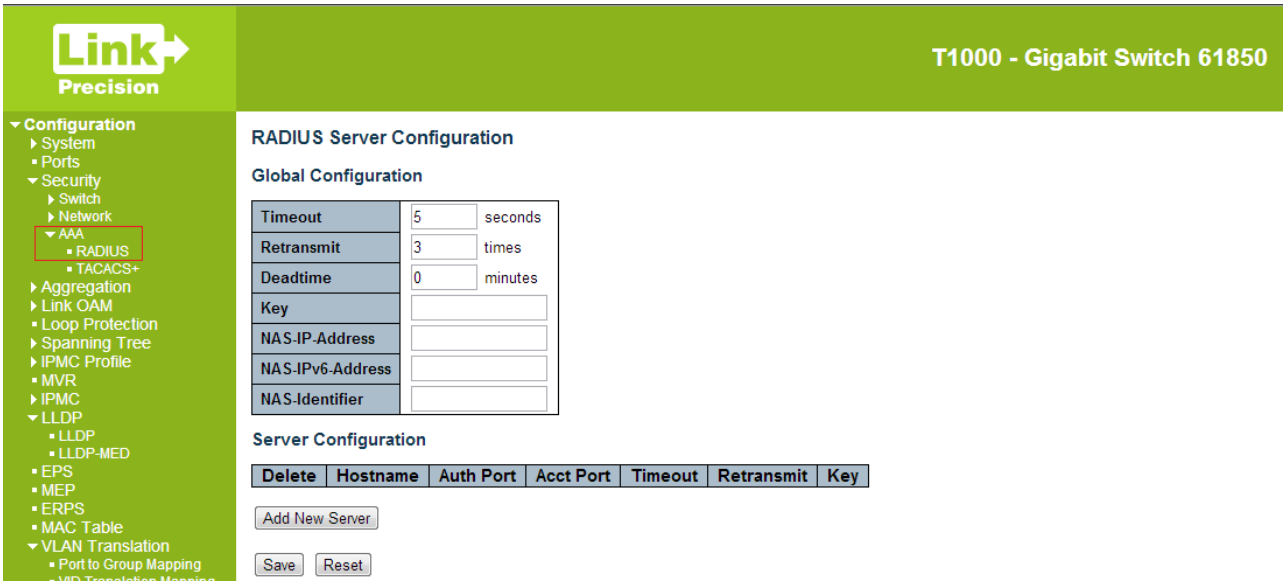
Buttons

AUTO REFRESH:Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Refreshes the displayed table starting from the input fields.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

|<<: Updates the table starting from the first entry in the Dynamic ARP Inspection Table.
>>: Updates the table, starting with the entry after the last entry currently displayed.

AAA

RADIUS Server Configuration



This page allows you to configure the RADIUS servers.

Global Configuration

These setting are common for all of the RADIUS servers.

Timeout

Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit

Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

Deadtime

Deadtime, which can be set to a number between 0 to 1440minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Key

The secret key - up to 63 characters long - shared between the RADIUS server and the switch.

NAS-IP-Address (Attribute 4)

The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-IPv6-Address (Attribute 9)

The IPv6 address to be used as attribute 9 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-Identifier (Attribute 32)

The identifier - up to 2 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Server Configuration

The table has one row for each RADIUS server and a number of columns, which are:

Delete

To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.

Hostname

The IP address or hostname of the RADIUS server.

Auth Port

The UDP port to use on the RADIUS server for authentication.

Acct Port

The UDP port to use on the RADIUS server for accounting.

Timeout

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Retransmit

This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

Key

This optional setting overrides the global key. Leaving it blank will use the global key.

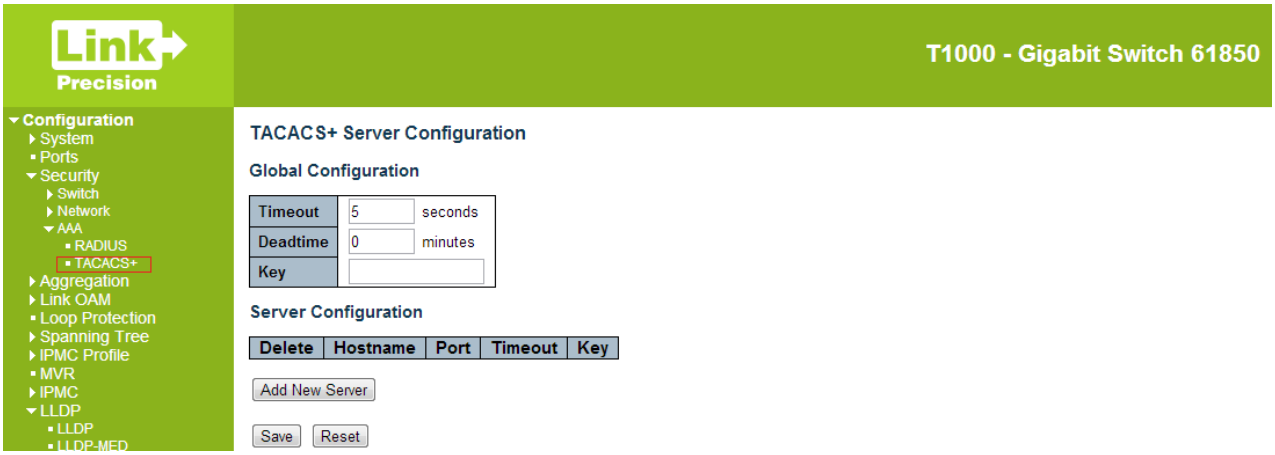
Adding a New Server

Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to servers are supported.
The button can be used to undo the addition of the new server.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

TACACS+ Server Configuration



This page allows you to configure the TACACS+ servers.

Global Configuration

These setting are common for all of the TACACS+ servers.

Timeout

Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.

Deadtime

Deadtime, which can be set to a number between 0 to 1440minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Key

The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration

The table has one row for each TACACS+ server and a number of columns, which are:

Delete

To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.

Hostname

The IP address or hostname of the TACACS+ server.

Port

The TCP port to use on the TACACS+ server for authentication.

Timeout

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Key

This optional setting overrides the global key. Leaving it blank will use the global key.

Adding a New Server

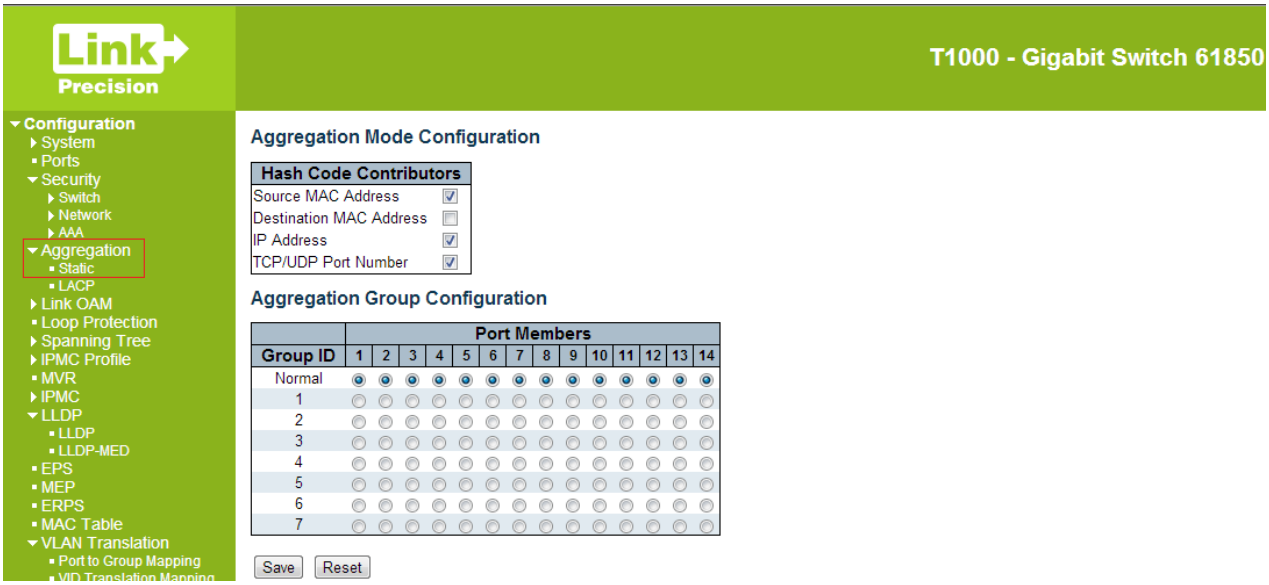
Click to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to servers are supported.
The button can be used to undo the addition of the new server.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

Aggregation

Aggregation Static Configuration



This page is used to configure the Aggregation hash mode and the aggregation group.

Hash Code Contributors

Source MAC Address

The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.

Destination MAC Address

The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.

IP Address

The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.

TCP/UDP Port Number

The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

Aggregation Group Configuration

Group ID

Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

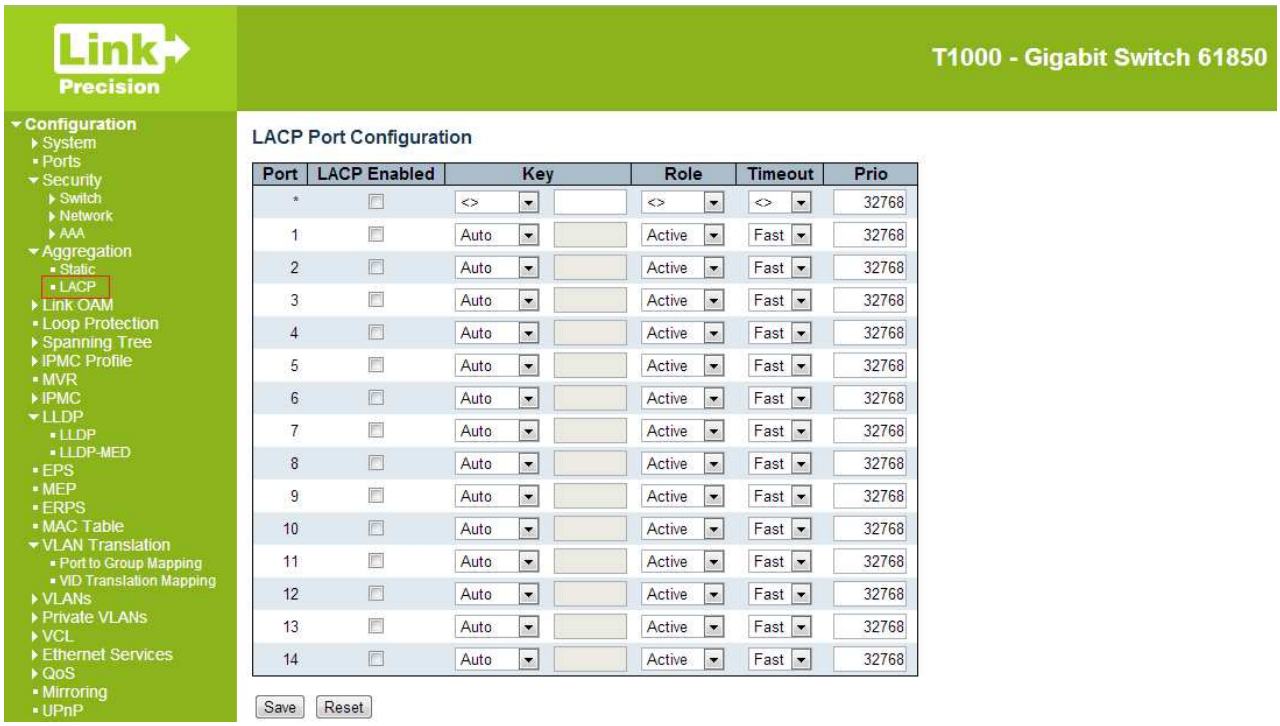
Port Members

Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

LACP Configuration



This page allows the user to inspect the current LACP port configurations, and possibly change them as well.

Port

The switch port number.

LACP Enabled

Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner.
Up to 32 aggregations are supported (if stackable).

Key

The Key value incurred by the port, range 1-63 . TheAuto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.

Role

The Role shows the LACP activity status. The Activewill transmit LACP packets each second, while Passivewill wait for a LACP packet from a partner (speak if spoken to).

Timeout

The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

Prio

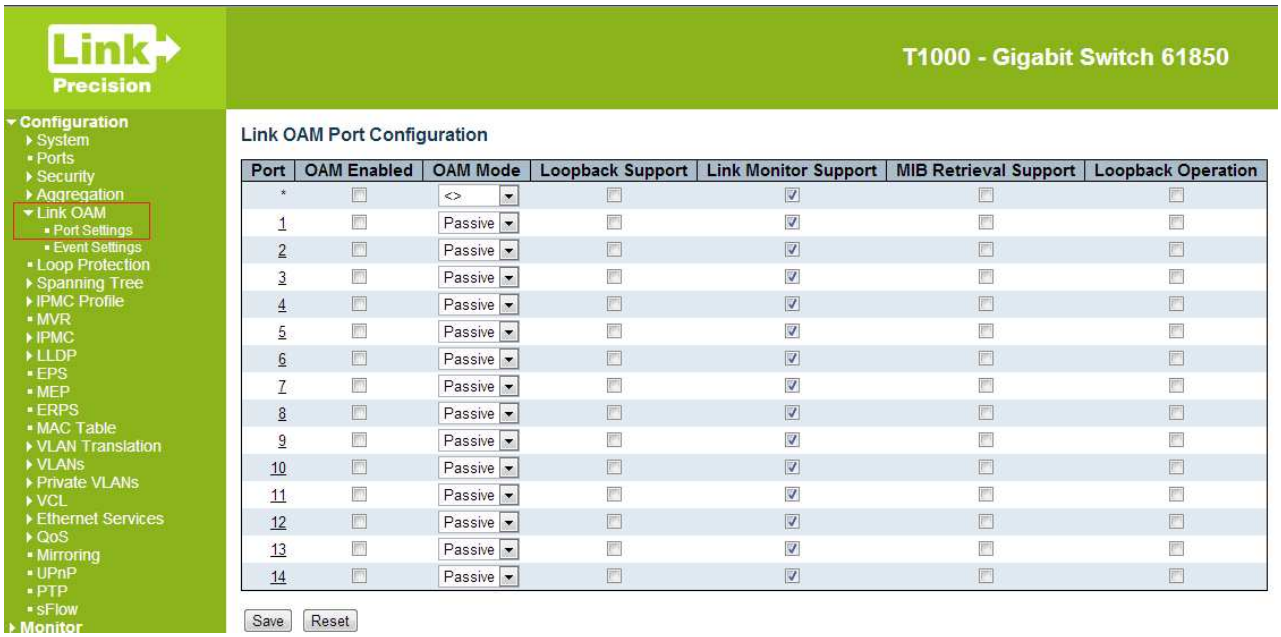
The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

Link OAM

Link OAM Port Configuration



This page allows the user to inspect the current Link OAM port configurations, and change them as well.

Port

The switch port number.

OAM Enabled

Controls whether Link OAM is enabled on this switch port. Enabling Link OAM provides the network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.

OAM Mode

Configures the OAM Mode as Active or Passive. The default mode is Passive.

Active mode

DTE's configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, Active DTE's are permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode. Active DTE's operate in a limited respect if the remote OAM entity is operating in Passive mode. Active devices should not respond to OAM remote loopback commands and variable requests from a Passive peer.

Passive mode

DTE's configured in Passive mode do not initiate the Discovery process. Passive DTE's react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive to passive links. Passive DTE's shall not send Variable Request or Loopback Control OAMPDUs.

Loopback Support

Controls whether the loopback support is enabled for the switch port. Link OAM remote loopback can be used for fault localization and link performance testing. Enabling the loopback support will allow the DTE to execute the remote loopback command that helps in the fault detection.

Link Monitor Support

Controls whether the Link Monitor support is enabled for the switch port. On enabling the Link Monitor support, the DTE supports event notification that permits the inclusion of diagnostic information.

MIB Retrieval Support

Controls whether the MIB Retrieval Support is enabled for the switch port. On enabling the MIB retrieval support, the DTE supports polling of various Link OAM based MIB variables' contents.

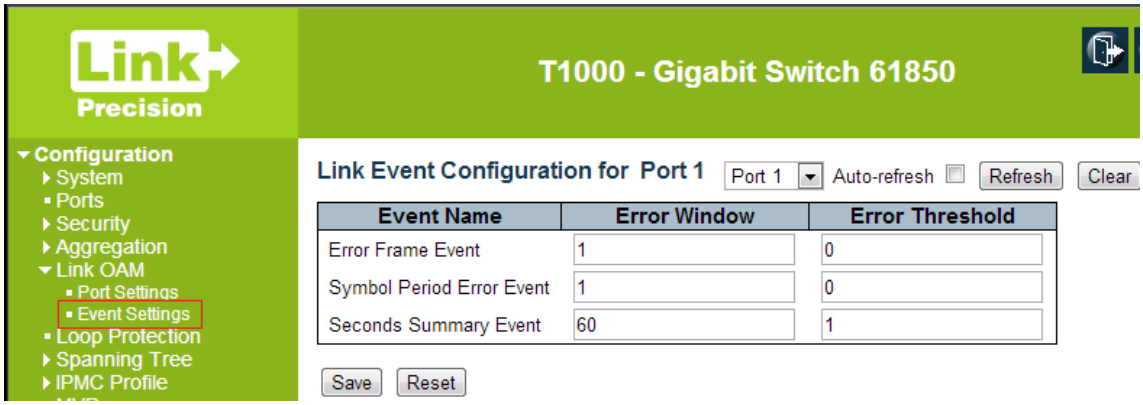
Loopback Operation

If the Loopback support is enabled, enabling this field will start a loopback operation for the port.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

Link OAM Link Event Configuration



This page allows the user to inspect the current Link OAM Link Event configurations, and change them as well.

Port

The switch port number.

Event Name

Name of the Link Event which is being configured.

Error Window

Represents the window period in the order of 1 sec for the observation of various link events.

Error Threshold

Represents the threshold value for the window period for the appropriate Link event so as to notify the peer of this error.

Error Frame Event

The Errored Frame Event counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 1 sec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Error Frame Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-0xffffffff and its default value is '0'.

Symbol Period Error Event

The Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. Error Window for 'Symbol Period Error Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-0xffffffff and its default value is '0'.

Seconds Summary Event

The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Seconds Summary Event' must be an integer value between 10-900 and its default value is '60'. Whereas Error Threshold must be between 0-0xffff and its default value is '1'.

Buttons

The port select box determines which port is affected by clicking the buttons.
AUTO-REFRESH : Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
CLEAR: Clears the counters for the selected port.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

Loop Protection

Loop Protection Configuration

This page allows the user to inspect the current Loop Protection configurations, and possibly change them as well.

General Settings

Enable Loop Protection

Controls whether loop protections is enabled (as a whole).

Transmission Time

The interval between each loop protection PDU sent on each port. valid values are 1 to 10 seconds.

Shutdown Time

The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).

Port Configuration

Port
The switch port number of the port.

Enable
Controls whether loop protection is enabled on this switch port.

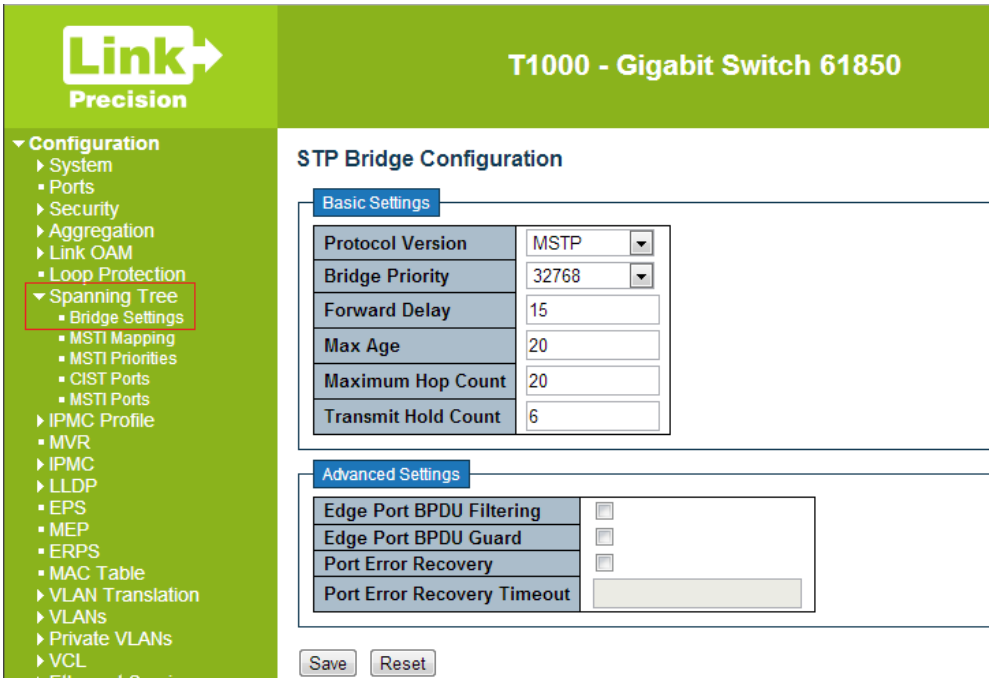
Action
Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port,Shutdown Port and Log or Log Only.

Tx Mode
Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

Spanning Tree

STP Bridge Configuration



This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch.

Basic Settings

Protocol Version

The MSTP / RSTP / STP protocol version setting. Valid values are STP, RSTP and MSTP.

Bridge Priority

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.
For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Forward Delay

The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age

The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

Maximum Hop Count

This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count

The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

Edge Port BPDU Filtering

Control whether a port explicitly configured as Edgewill transmit and receive BPDUs.

Edge Port BPDU Guard

Control whether a port explicitly configured as Edgewill disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Port Error Recovery

Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

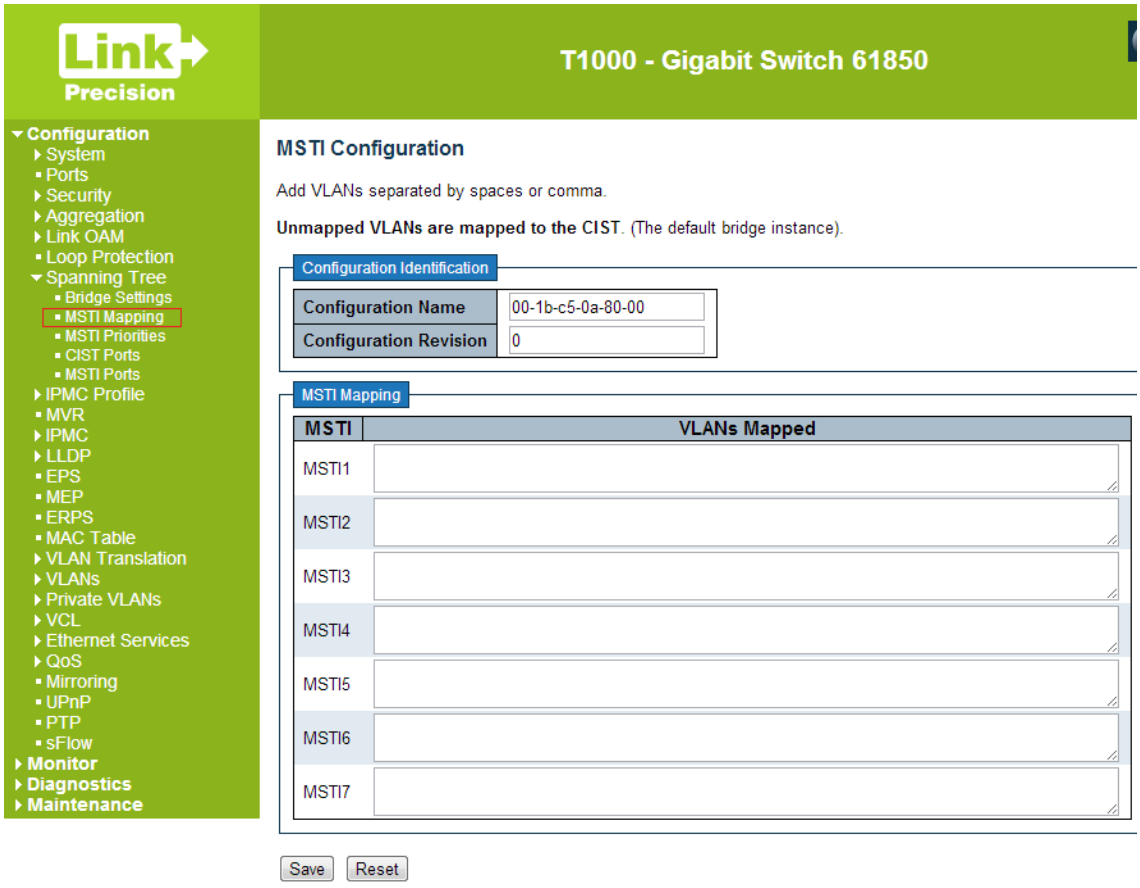
Port Error Recovery Timeout

The time to pass before a port in the error-disabledstate can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

STP MSTI Configuration



This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

Configuration Identification

Configuration Name

The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision

The revision of the MSTI configuration named above. This must be an integer between 0 and 63.

MSTI Mapping

MSTI

The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

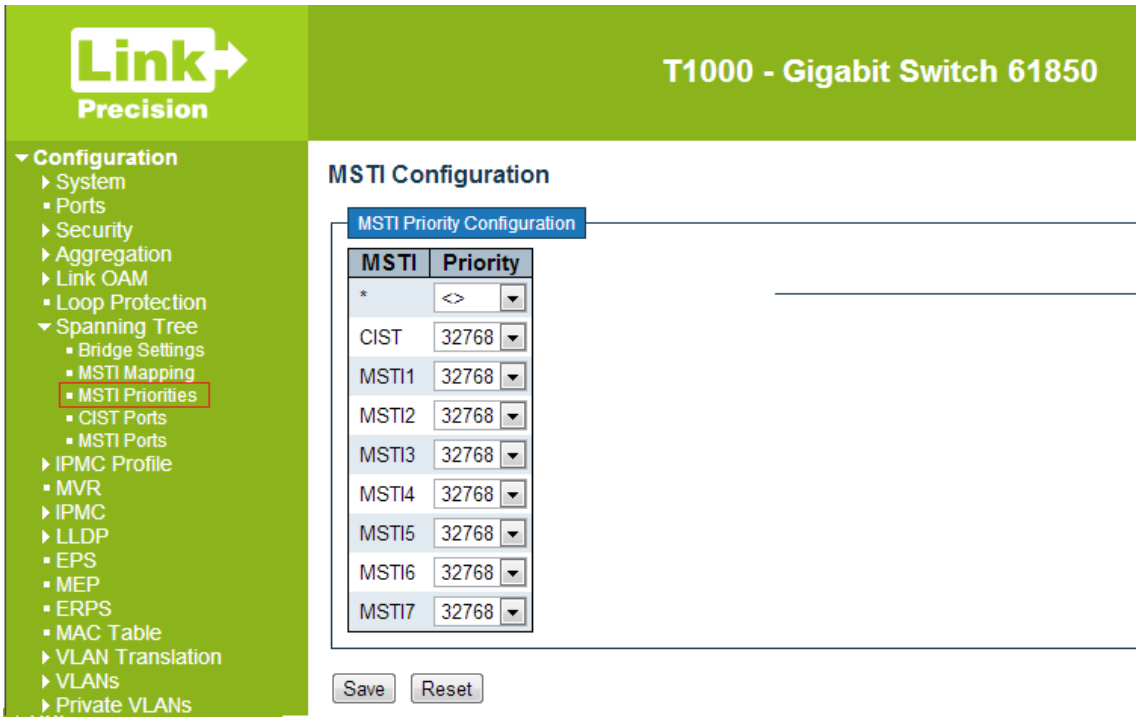
VLANs Mapped

The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: 2,,20-40.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

STP MSTI Priority Configuration



This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

MSTI

The bridge instance. The CIST is the default instance, which is always active.

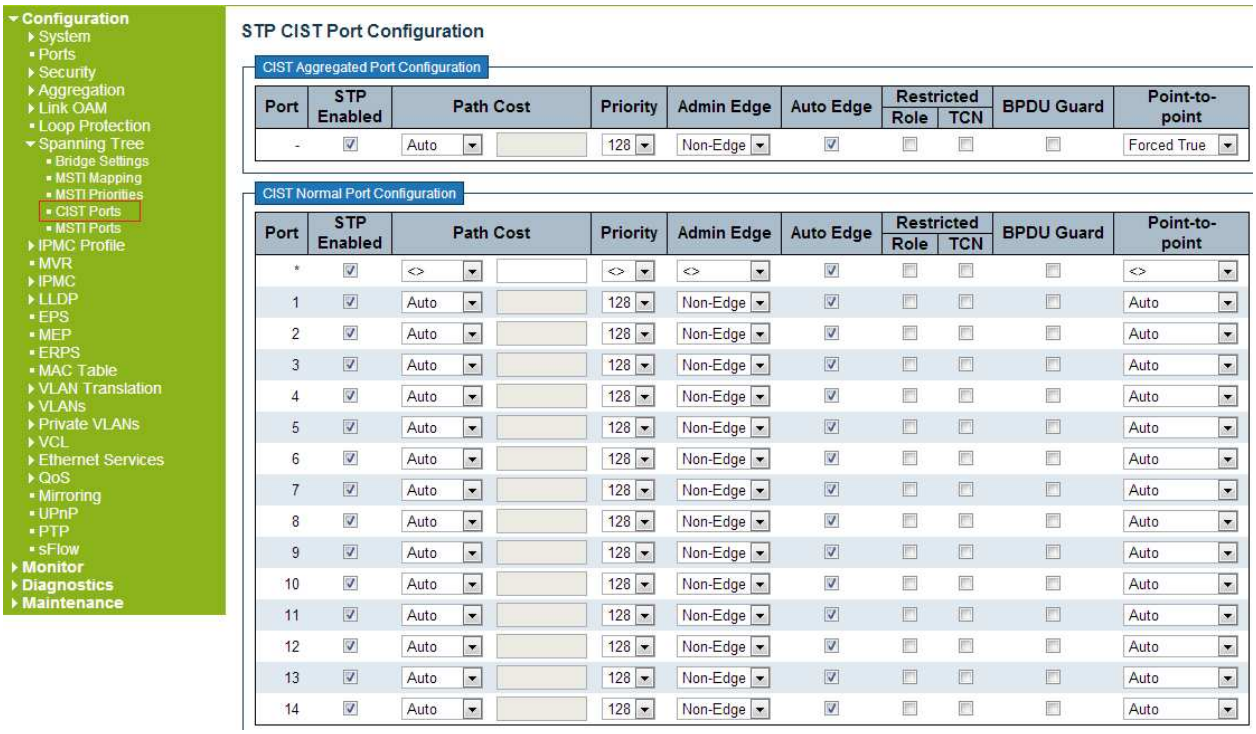
Priority

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

STP CIST Port Configuration



This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well.
This page contains settings for physical and aggregated ports.

Port

The switch port number of the logical STP port.

STP Enabled

Controls whether STP is enabled on this switch port.

Path Cost

Controls the path cost incurred by the port. The Autosetting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority

Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

operEdge (state flag)

Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (havingoperEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

AdminEdge

Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).

AutoEdge

Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restricted Role

If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restricted TCN

If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard

If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the portEdge status does not effect this setting.
A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

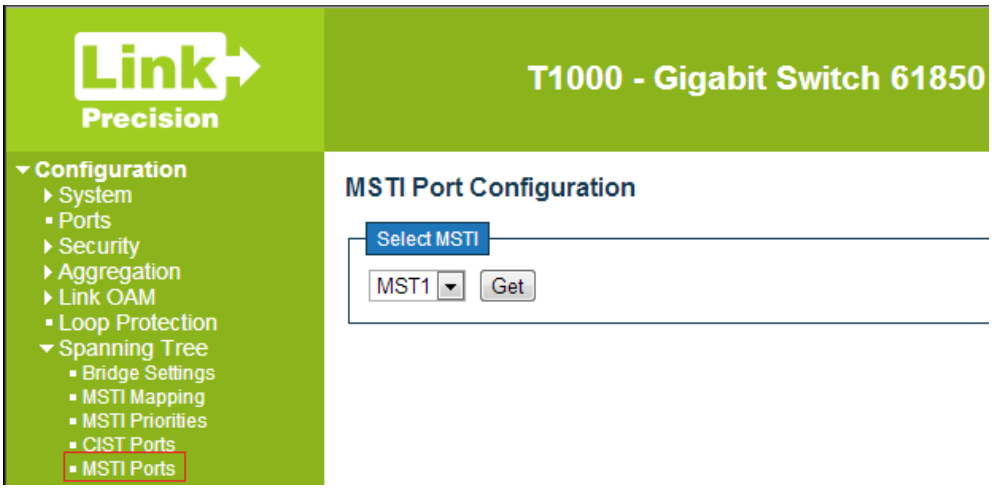
Point-to-Point

Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

STP MSTI Port Configuration



This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well.
An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.
This page contains MSTI port settings for physical andaggregated ports.

Port

The switch port number of the corresponding STP CIST (and MSTI) port.

Path Cost

Controls the path cost incurred by the port. The Autosetting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority

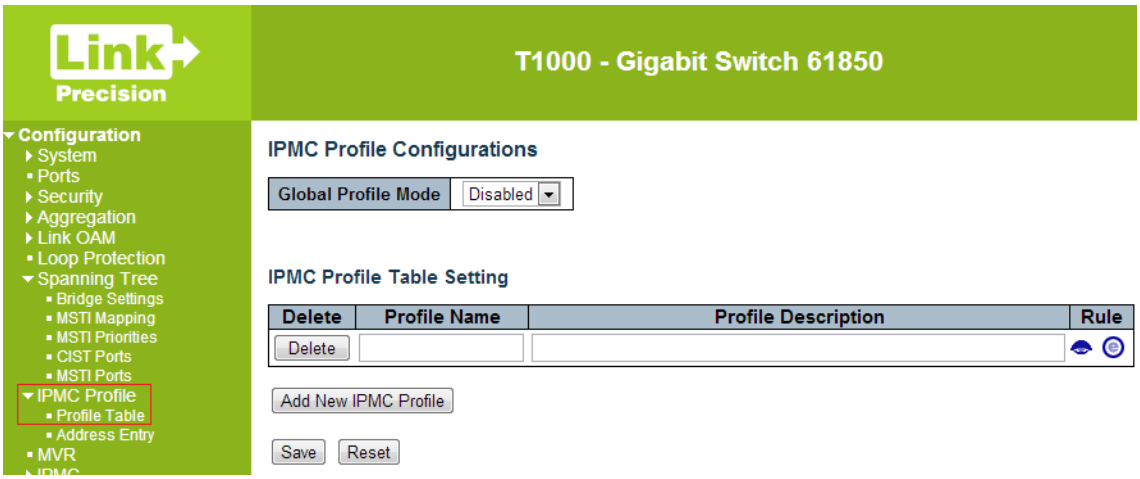
Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

Buttons

GET: Click to retrieve settings for a specific MSTI.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

IPMC Profile

IPMC Profile Configurations



This page provides IPMC Profile related configurations.
The IPMC profile is used to deploy the access control on IPmulticast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.

Global Profile Mode

Enable/Disable the Global IPMC Profile.
System starts to do filtering based on profile settings only when the global profile mode is enabled.

Delete

Check to delete the entry.
The designated entry will be deleted during the next save.

Profile Name

The name used for indexing the profile table.
Each entry has the unique name which is composed of at maximun 16 alphabetic and numeric characters. At least one alphabet must be present.

Profile Description

Additional description, which is composed of at maximun 64 alphabetic and numeric characters, about the profile.
No blank or space characters are permitted as part of description. Use "_" or "-" to seperate the description sentence.

Rule

When the profile is created, click the edit button to enter the rule setting page of the designated profile.
Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons:

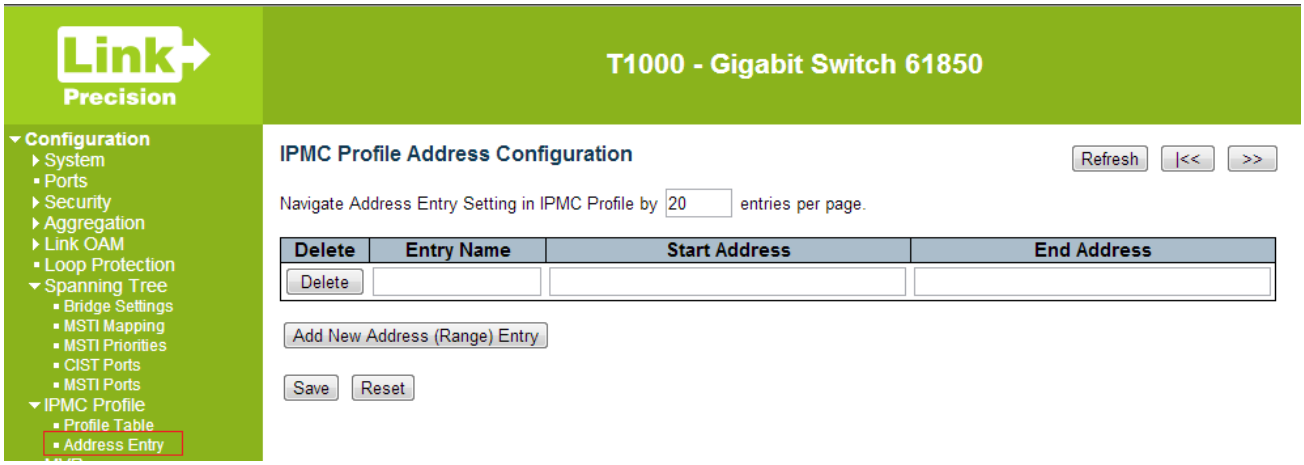
: List the rules associated with the designated profile.

: Adjust the rules associated with the designated profile.

Buttons

ADD NEW IPMC PROFILE: Click to add new IPMC profile. Specify the name and configure the new entry. Click "Save".
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

IPMC Profile Address Entry Table



This page provides address range settings used in IPMC profile.
The address entry is used to specify the address range that will be associated with IPMC Profile. It is allowed to create at maximum 128 address entries in the system.

Delete

Check to delete the entry.
The designated entry will be deleted during the next save.

Entry Name

The name used for indexing the address entry table.
Each entry has the unique name which is composed of at maximun 16 alphabetic and numeric characters. At least one alphabet must be present.

Start Address

The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.

End Address

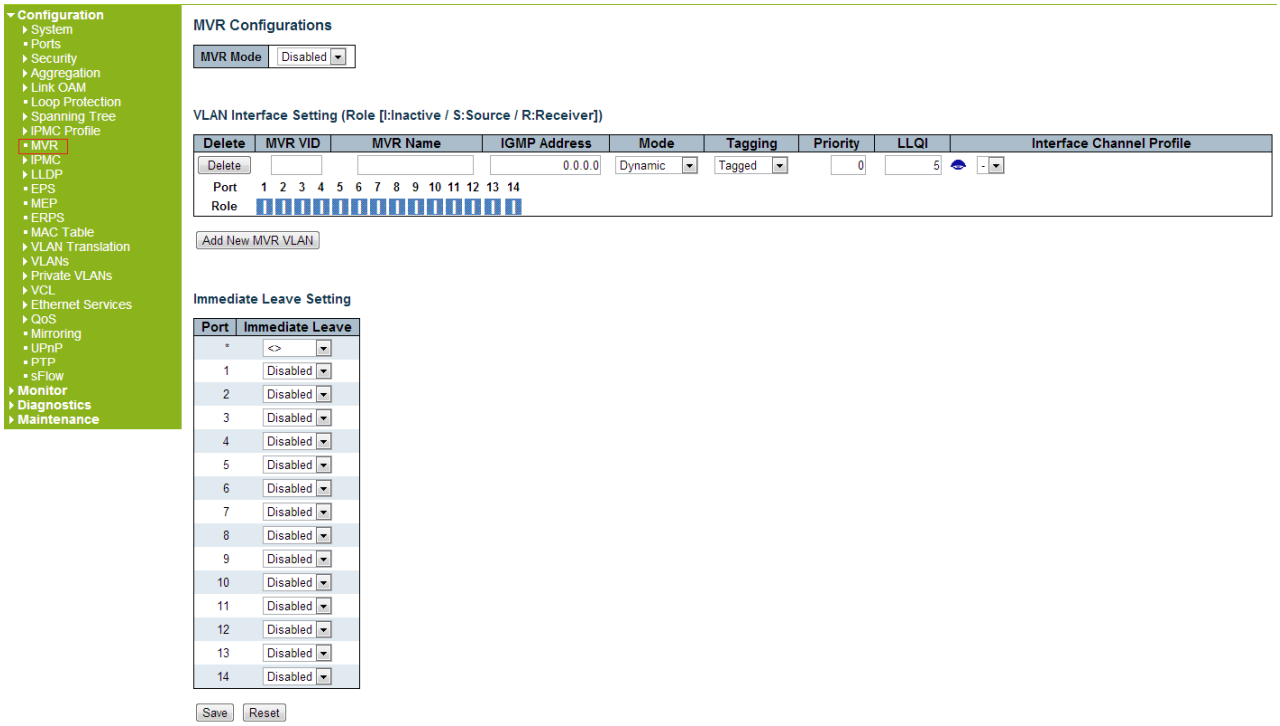
The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Buttons

ADD NEW ADDRESS (RANGE) ENTRY: Click to add new address range. Specify the name and configure the addresses. Click "Save"
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.
REFRESH: Refreshes the displayed table starting from the input fields.
|<<: Updates the table starting from the first entry in the IPMC Profile Address Configuration.
>>: Updates the table, starting with the entry after the last entry currently displayed.

MVR

MVR Configurations



This page provides MVR related configurations.
The MVR feature enables multicast traffic forwarding on the Multicast VLANs. In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports. It is allowed to create at maximum 8 MVR VLANs with corresponding channel settings for each Multicast VLAN. There will be totally at maximum 26 group addresses for channel settings.

MVR Mode

Enable/Disable the Global MVR.
The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping.
It is suggested to enable Unregistered Flooding control when the MVR group table is full.

Delete

Check to delete the entry. The designated entry will be deleted during the next save.

MVR VID

Specify the Multicast VLAN ID.

Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

MVR Name

MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

IGMP Address

Define the IPv4 address as source address used in IP header for IGMP control frames.
When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.
When the IPv4 management address is not set, system uses the first available IPv4 management address.
Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Mode

Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.

Tagging

Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.

Priority

Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

LLQI

Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is tenths or one-half second.

Interface Channel Profile

When the MVR VLAN is created, select the IPMC Profile as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view button. Profile selected for designated interface channel is not allowed to have overlapped permit group address.

Profile Management Button

You can inspect the rules of the designated profile by using the following button:
: List the rules associated with the designated profile.

Port

The logical port for the settings.

Port Role

Configure an MVR port of the designated MVR VLAN as one of the following roles.
Inactive: The designated port does not participate MVR operations.
Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.
Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.
Select the port role by clicking the Role symbol to switch the setting.
I indicates Inactive; S indicates Source; R indicates Receiver
The default Role is Inactive.

Immediate Leave

Enable the fast leave on the port.

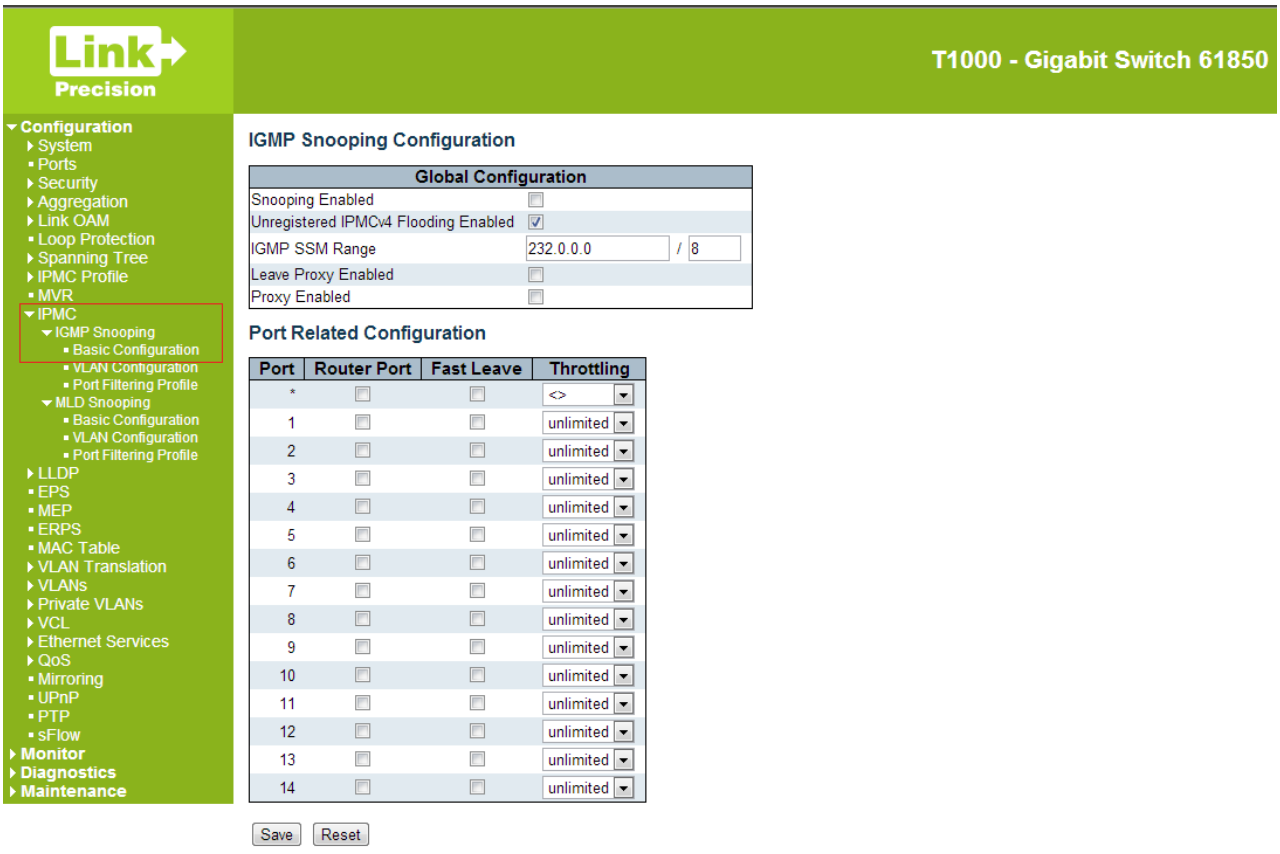
Buttons

ADD NEW MVR VLAN: Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Save".
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

IPMC

IGMP Snooping

IGMP Snooping Configuration



This page provides IGMP Snooping related configuration.

Snooping Enabled

Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding Enabled

Enable unregistered IPMCv4 traffic flooding.
The flooding control takes effect only when IGMP Snooping is enabled.
When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.

IGMP SSM Range

SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Leave Proxy Enabled

Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled

Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.
If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.

Throttling

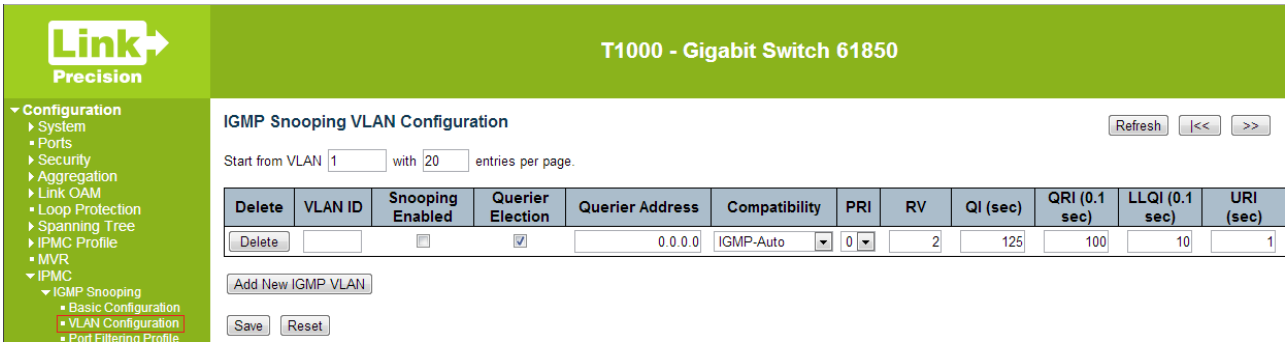
Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

I

IGMP Snooping VLAN Configuration



Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the next closest VLAN Table match.
The will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

IGMP Snooping VLAN Table Columns

Delete
Check to delete the entry. The designated entry will be deleted during the next save.

VLAN ID
The VLAN ID of the entry.

IGMP Snooping Enabled
Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.

Querier Election
Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address
Define the IPv4 address as source address used in IP header for IGMP Querier election.
When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.
When the IPv4 management address is not set, system uses the first available IPv4 management address.
Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Compatibility
Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network.
The allowed selection is IGMP-Auto, Forced IGMPv1,Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

PRI
Priority of Interface.
It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

RV

Robustness Variable.
The Robustness Variable allows tuning for the expected packet loss on a network.
The allowed range is 1 to 2, default robustness variable value is 2.

QI

Query Interval.
The Query Interval is the interval between General Queries sent by the Querier.
The allowed range is 1 to 31744 seconds, default query interval is 12 seconds.

QRI

Query Response Interval.
The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.
The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP)

Last Member Query Interval.
The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count.
The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).

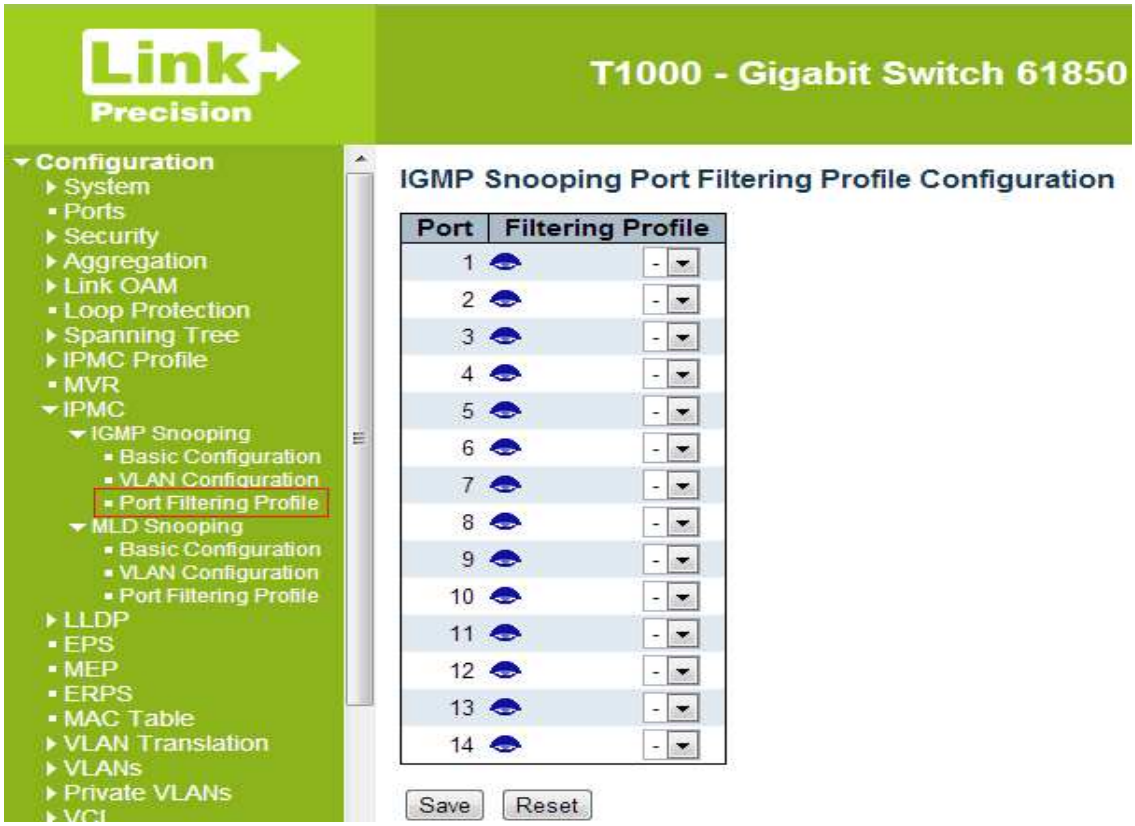
URI

Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group.
The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons

REFRESH: Refreshes the displayed table starting from the "VLAN" input fields.
|<<: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
>>: Updates the table, starting with the entry after the last entry currently displayed.
ADD NEW IGMP VLAN: Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

IGMP Snooping Port Filtering Profile Configuration



Port

The logical port for the settings.

Filtering Profile

Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Profile Management Button

You can inspect the rules of the designated profile by using the following button:

: List the rules associated with the designated profile.

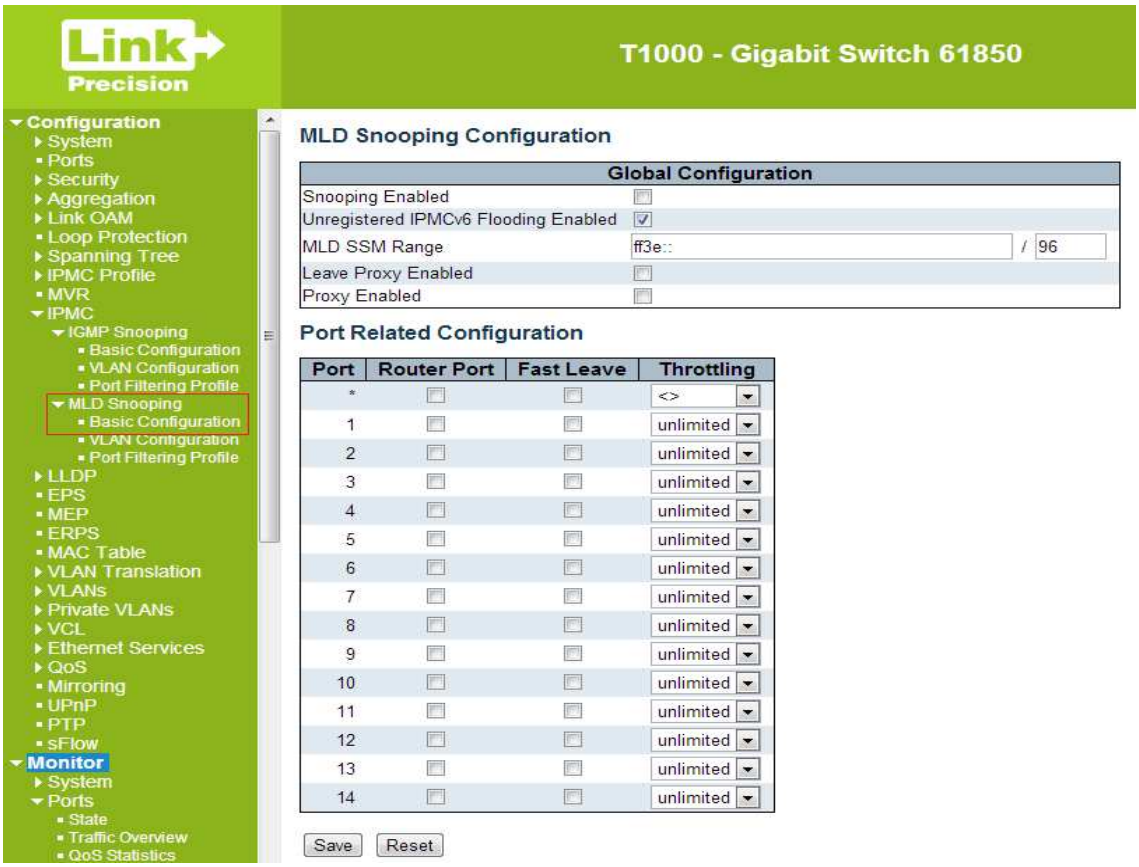
Buttons

SAVE: Click to save changes.

RESET: Click to undo any changes made locally and revert to previously saved values.

MLD Snooping

MLD Snooping Configuration



This page provides MLD Snooping related configuration.

Snooping Enabled

Enable the Global MLD Snooping.

Unregistered IPMCv6 Flooding Enabled

Enable unregistered IPMCv6 traffic flooding.
The flooding control takes effect only when MLD Snooping is enabled.
When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

MLD SSM Range

SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Leave Proxy Enabled

Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled

Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.
If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.

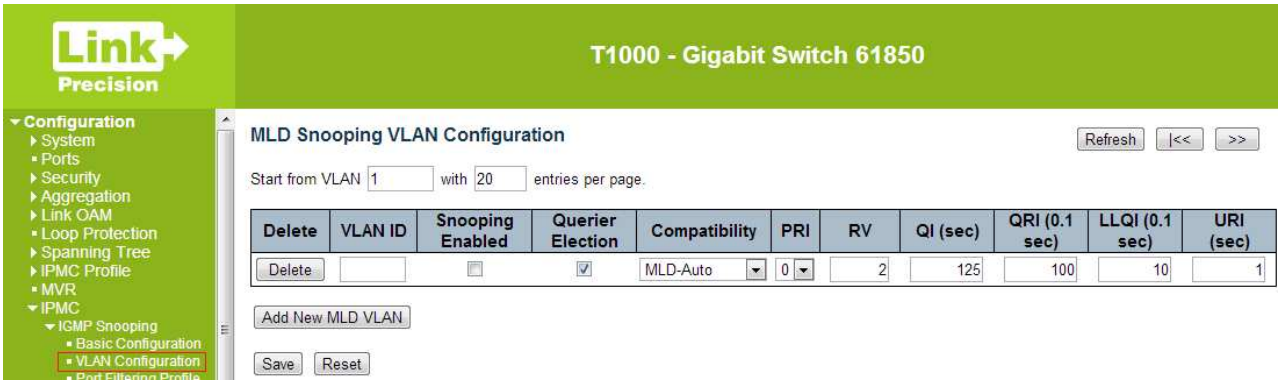
Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

MLD Snooping VLAN Configuration



Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the next closest VLAN Table match.
The will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

MLD Snooping VLAN Table Columns

Delete
Check to delete the entry. The designated entry will be deleted during the next save.

VLAN ID
The VLAN ID of the entry.

MLD Snooping Enabled
Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.

Querier Election
Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.

Compatibility
Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network.
The allowed selection is MLD-Auto, Forced MLDv1,Forced MLDv2, default compatibility value is MLD-Auto.

PRI
Priority of Interface.
It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.
The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

RV
Robustness Variable.
The Robustness Variable allows tuning for the expected packet loss on a link.

The allowed range is 1 to 2, default robustness variable value is 2.

QI
Query Interval.
The Query Interval is the interval between General Queries sent by the Querier.
The allowed range is 1 to 31744 seconds, default query interval is 12 seconds.

QRI
Query Response Interval.
The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.
The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

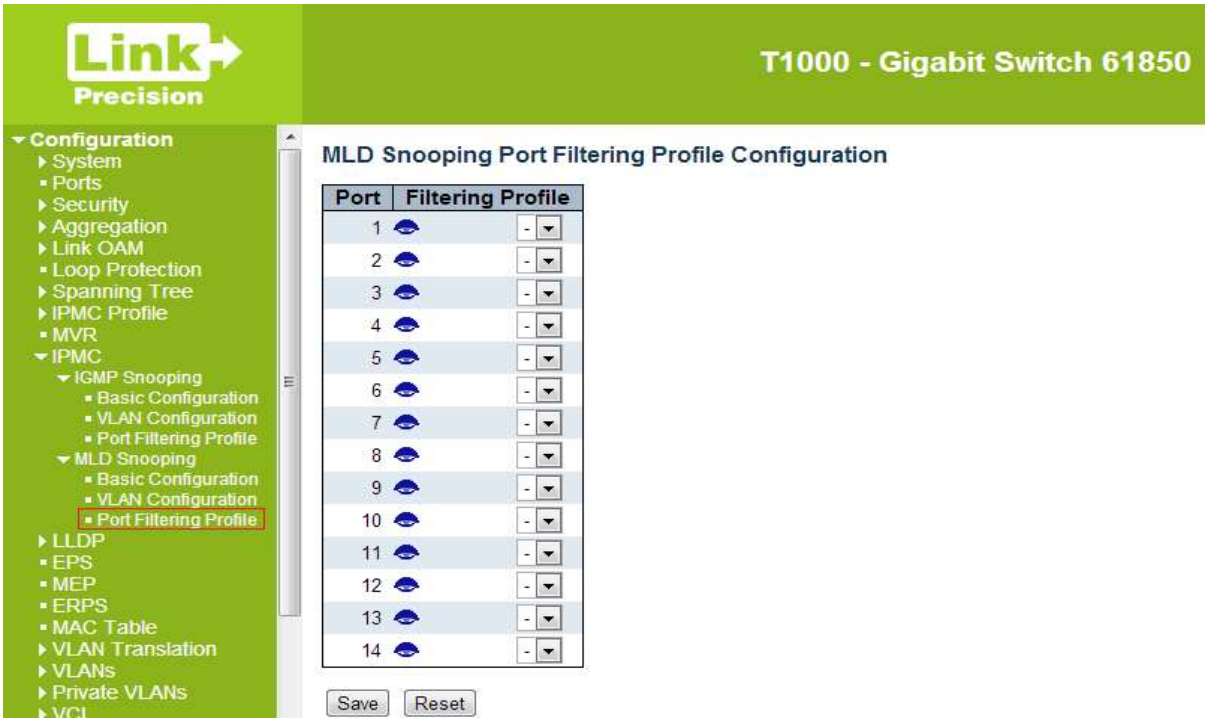
LLQI
Last Listener Query Interval.
The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages.
The allowed range is 0 to 31744 in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second).

URI
Unsolicited Report Interval.
The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address.
The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons

REFRESH: Refreshes the displayed table starting from the "VLAN" input fields.
|<<: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
>>: Updates the table, starting with the entry after the last entry currently displayed.
ADD NEW MLD VLAN: Click to add new MLD VLAN. Specify the VID and configure the new entry. Click "Save". The specific MLD VLAN starts working after the corresponding static VLAN is also created.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

MLD Snooping Port Filtering Profile Configuration



Port

The logical port for the settings.

Filtering Profile

Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Profile Management Button

You can inspect the rules of the designated profile by using the following button:

: List the rules associated with the designated profile.

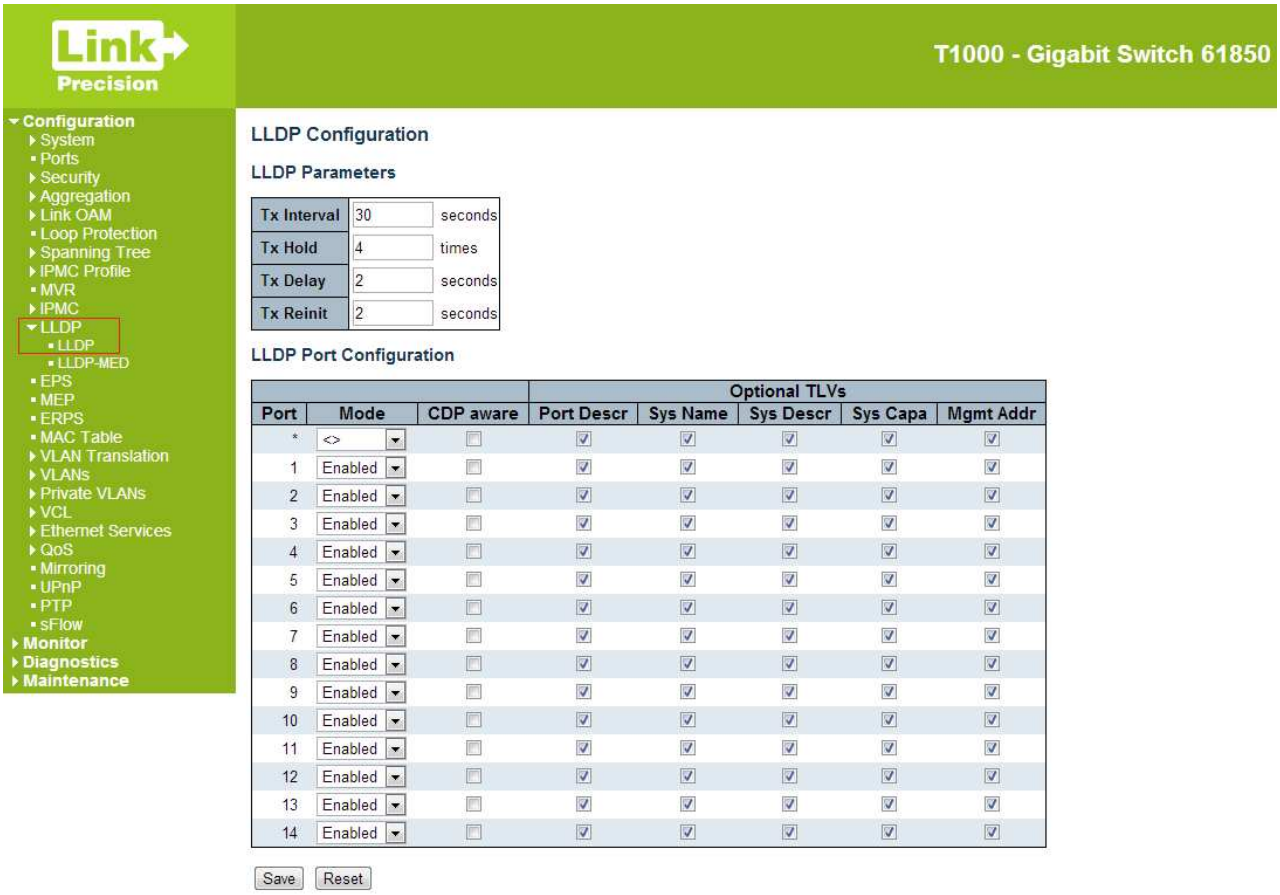
Buttons

SAVE: Click to save changes.

RESET: Click to undo any changes made locally and revert to previously saved values.

LLDP

LLDP Configuration



This page allows the user to inspect and configure the currentLLDP port settings.

LLDP Parameters

Tx Interval

The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to - 32768 seconds.

Tx Hold

Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Holdmultiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.

Tx Delay

If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between theLLDP frames will always be at least the value of Tx Delayseconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.

Tx Reinit

When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signalling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

Port

The switch port number of the logical LLDP port.

Mode

Select LLDP mode.
Rx only The switch will not send out LLDP information, but LLDP information from neighbour units is analyzed.
Tx only The switch will drop LLDP information received from neighbours, but will send out LLDP information.
Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbours.
Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbours.

CDP Aware

Select CDP awareness.
The CDP operation is restricted to decoding incoming CDPframes (The switch doesn't transmit CDP frames). CDPframes are only decoded if LLDP on the port is enabled.
Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbours' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbours' table as shown below.
CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.
CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDPneighbours table.
CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.
CDP TLV "Version and Platform" is mapped to the LLDP"System Description" field.
Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in theLLDP neighbours' table.
If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbour devices. If at least one port has CDP awareness enabled all CDPframes are terminated by the switch.
Note: When CDP awareness on a port is disabled the CDPinformation isn't removed immediately, but gets removed when the hold time is exceeded.

Port Descr

Optional TLV: When checked the "port description" is included in LLDP information transmitted.

Sys Name

Optional TLV: When checked the "system name" is included in LLDP information transmitted.

Sys Descr

Optional TLV: When checked the "system description" is included in LLDP information transmitted.

Sys Capa

Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

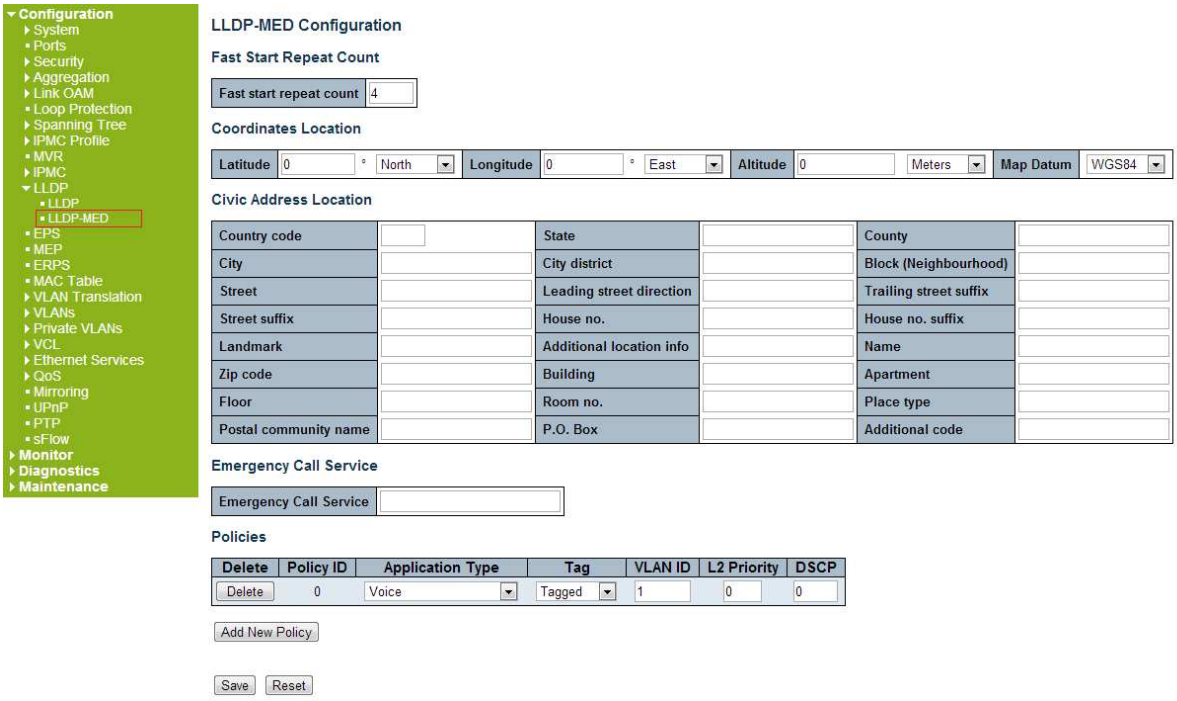
Mgmt Addr

Optional TLV: When checked the "management address" is included in LLDP information transmitted.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

LLDP Media Configuration



This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

Fast start repeat count

Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbour has been detected in order share LLDP-MED information as fast as possible to new neighbours.

Because there is a risk of an LLDP frame being lost during transmission between neighbours, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbours receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not

apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

Coordinates Location

Latitude

Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits.
It is possible to specify the direction to either North of the equator or South of the equator.

Longitude

Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits.
It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

Altitude

Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits.
It is possible to select between two altitude types (floors or meters).
Meters: Representing meters of Altitude defined by the vertical datum specified.
Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

Map Datum

The Map Datum is used for the coordinates given in these options:
WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.
NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).
NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Country code

The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

State

National subdivisions (state, canton, region, province, prefecture).

County

County, parish, gun (Japan), district.

City

City, township, shi (Japan) - Example: Copenhagen.

City district

City division, borough, city district, ward, chou (Japan).

Block (Neighbourhood)

Neighbourhood, block.

Street

Street - Example: Poppelvej.

Leading street direction
Leading street direction - Example: N.

Trailing street suffix
Trailing street suffix - Example: SW.

Street suffix
Street suffix - Example: Ave, Platz.

House no.
House number - Example: 21.

House no. suffix
House number suffix - Example: A, 1/2.

Landmark
Landmark or vanity address - Example: Columbia University.

Additional location info
Additional location info - Example: South Wing.

Name
Name (residence and office occupant) - Example: Flemming Jahn.

Zip code
Postal/zip code - Example: 2791.

Building
Building (structure) - Example: Low Library.

Apartment
Unit (Apartment, suite) - Example: Apt 42.

Floor
Floor - Example: 4.

Room no.
Room number - Example: 40F.

Place type
Place type - Example: Office.

Postal community name
Postal community name - Example: Leonia.

P.O. Box
Post office box (P.O. BOX) - Example: 1234.

Additional code
Additional code - Example: 1320300003.

Emergency Call Service

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Emergency Call Service

Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.
Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.
The network policy attributes advertised are:
1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)
This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:
1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
. Streaming Video
6. Control / Signalling (conditionally support a separate network policy for the media types above)
A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.
It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Delete

Check to delete the policy. It will be deleted during the next save.

Policy ID

ID for the policy. This is auto generated and shall be used when selecting the polices that shall be mapped to the specific ports.

Application Type

Intended use of the application types:
1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. Voice Signalling (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.
3. Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. Guest Voice Signalling (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voiceapplication policy.

. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.
6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video Signalling (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencingapplication policy.

Tag
Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.
Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.
Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

VLAN ID
VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.

L2 Priority
L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

DSCP
DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 247.

Adding a new policy
Click to add a new policy. Specify theApplication type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save".
The number of policies supported is 32

Port Policies Configuration
Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

Port
The port number to which the configuration applies.

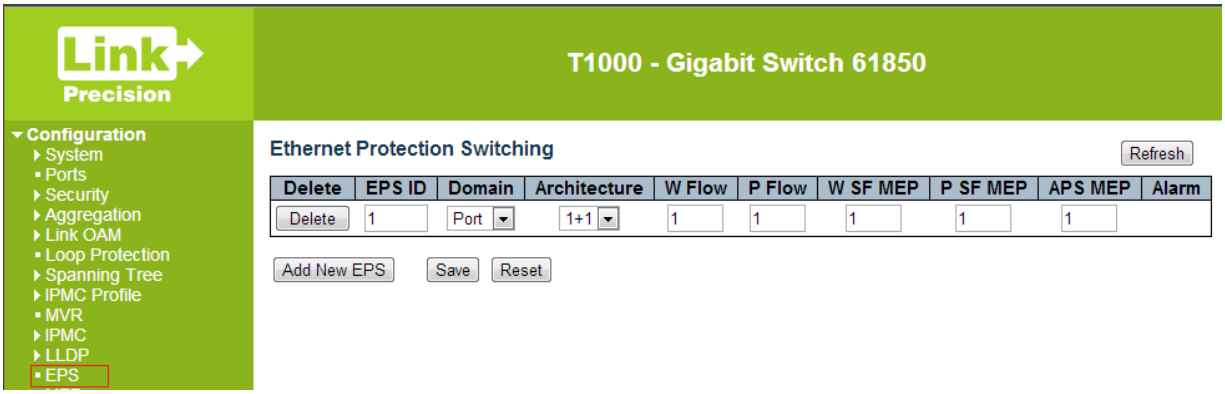
Policy ID
The set of policies that shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

EPS

EPS Configuration



The Ethernet (Linear) Protection Switch instances are configured here.

Delete

This box is used to mark an EPS for deletion in next Save operation.

EPS ID

The ID of the EPS. Click on the ID of an EPS to enter the configuration page.

Domain

Port: This will create a EPS in the Port Domain. 'W/P Flow' is a Port.
Esp: Future use
Evc: This will create a EPS in the EVC Domain. 'W/P Flow' is a EVC
Mpls: Future use

Architecture

Port: This will create a 1+1 EPS.
Port: This will create a 1:1 EPS.

W Flow

The working flow for the EPS - See 'Domain'.

P Flow

The protecting flow for the EPS - See 'Domain'.

W SF MEP

The working Signal Fail reporting MEP.

P SF MEP

The protecting Signal Fail reporting MEP.

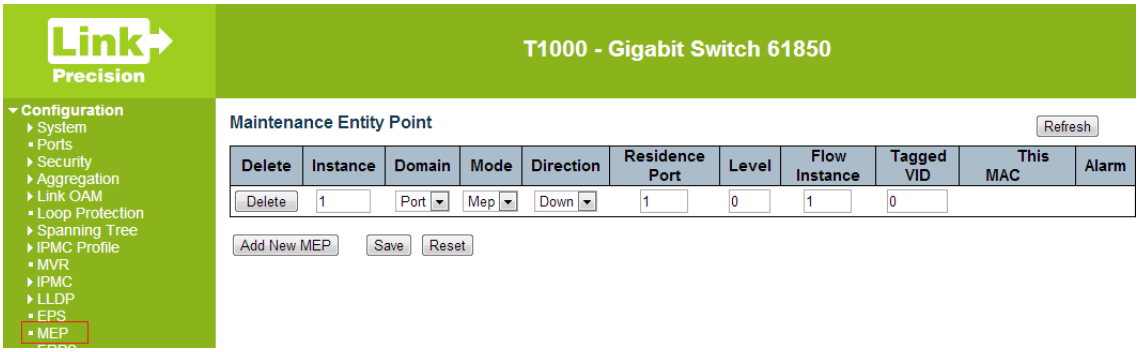
APS MEP
The APS PDU handling MEP.

Alarm
There is an active alarm on the EPS.

Buttons
ADD NEW EPS: Click to add a new EPS entry.
REFRESH: Click to refresh the page immediately.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

MEP

MEP Configuration



The Maintenance Entity Point instances are configured here.

Delete

This box is used to mark a MEP for deletion in next Save operation.

Instance

The ID of the MEP. Click on the ID of a MEP to enter the configuration page.

Domain

Port: This is a MEP in the Port Domain. 'Flow Instance' is a Port.
Evc: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC

Mode

MEP: This is a Maintenance Entity End Point.
MIP: This is a Maintenance Entity Intermediate Point.

Direction

Up: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.
Down: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

Residence Port

The port where MEP is monitoring - see 'Direction'.

Level

The MEG level of this MEP.

Flow Instance

The MEP is related to this flow - See 'Domain'.

Tagged VID

Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.
EVC MIP: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.

This MAC

The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Alarm

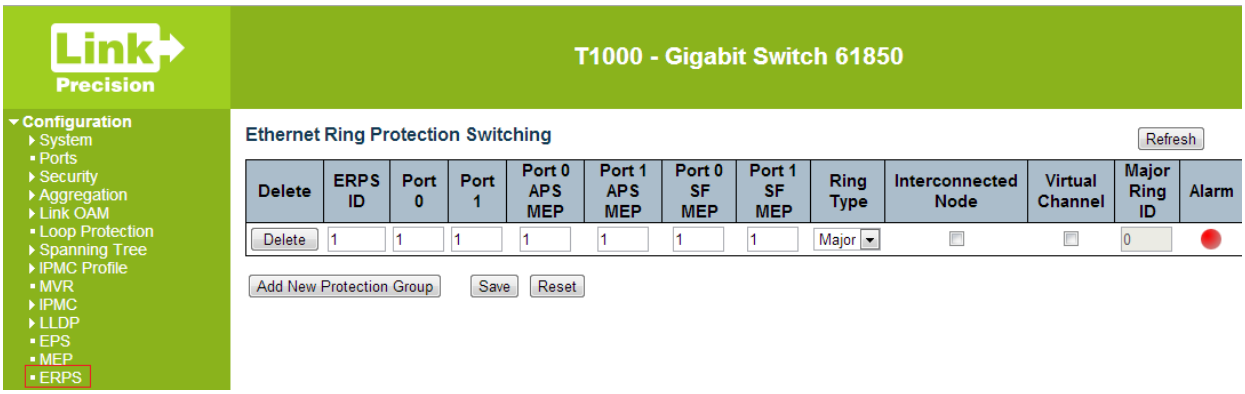
There is an active alarm on the MEP.

Buttons

ADD A NEW MEP: Click to add a new MEP entry.
REFRESH: Click to refresh the page immediately.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

ERPS

ERPS Configuration



The Ethernet Ring Protection Switch instances are configured here.

Delete

This box is used to mark an ERPS for deletion in next Save operation.

Protection group ID

The ID of the created Protection group. Click on the ID of an Protection group to enter the configuration page.

Port 0

This will create a Port 0 of the switch in the ring.

Port 1

This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance

Port 0 SF MEP

The Port 0 Signal Fail reporting MEP.

Port 1 SF MEP

The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.

Port 0 APS MEP

The Port 0 APS PDU handling MEP.

Port 1 APS MEP

The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type

Type of Protecting ring. It can be either major ring or sub-ring.

Interconnected Node

Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.

Virtual Channel

Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel.

Major Ring ID

Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.

Alarm

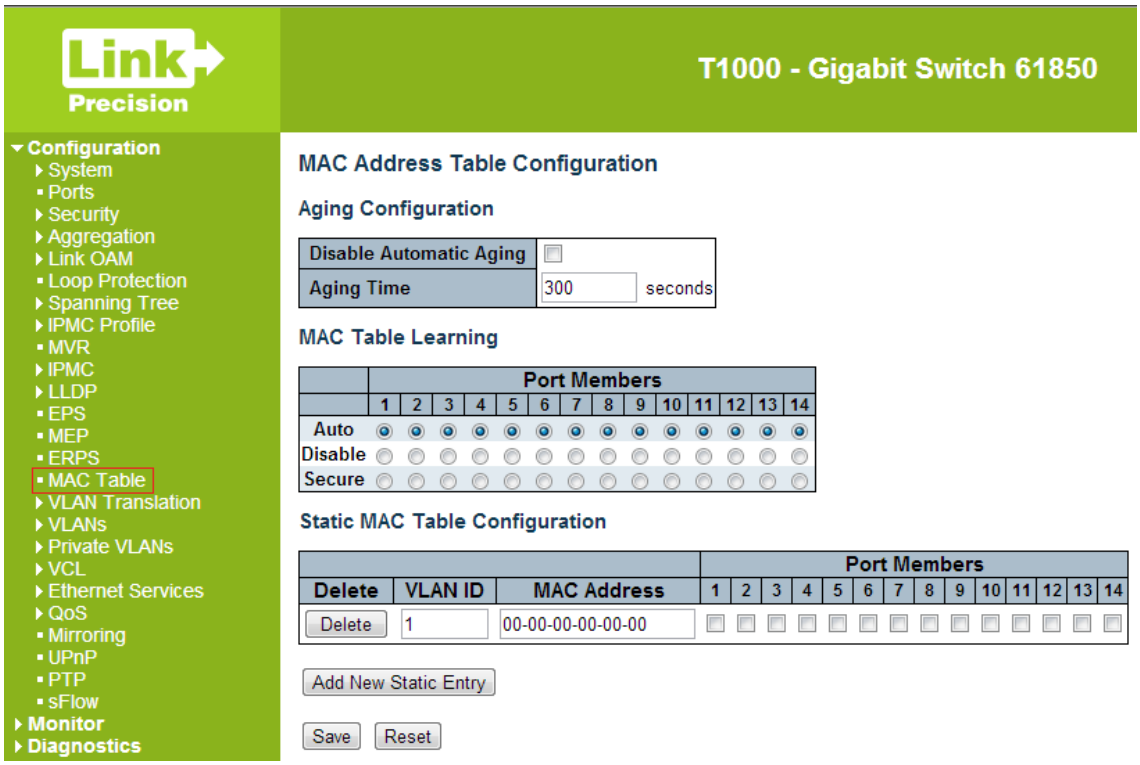
There is an active alarm on the ERPS.

Buttons

ADD NEW PROTECTION GROUP: Click to add a new Protection group entry.
REFRESH: Click to refresh the page immediately.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

MAC Table

MAC Address Table Configuration



The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds; for example, Age time seconds.

The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking Disable automatic aging.

MAC Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Each port can do learning based upon the following settings:

Auto

Learning is done automatically as soon as a frame with unknown SMAC is received.

Disable
No learning is done.

Secure
Only static MAC entries are learned, all other frames are dropped.
Note: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration
The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The MAC table is sorted first by VLAN ID and then by MAC address.

Delete
Check to delete the entry. It will be deleted during the next save.

VLAN ID
The VLAN ID of the entry.

MAC Address
The MAC address of the entry.

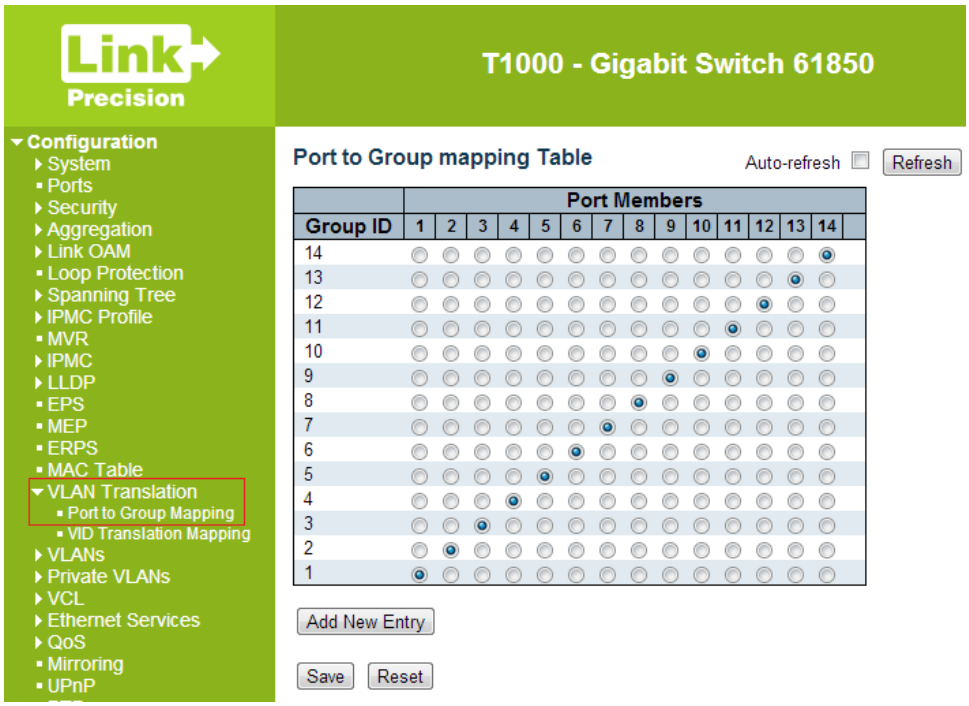
Port Members
Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Adding a New Static Entry
Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

Buttons
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

VLAN Translation

Port to Group mapping Table



This page allows you to map set of Port members to a Group ID for all switch ports.
The displayed settings are:

Group ID

A valid Group ID is an integer value form 1 to 14. A set of VLAN Translations are mapped to a group Id. This way a port is mapped to a list of VLAN Translations easily by mapping it to a group. Number of groups in this switch is equal to the number of ports (14) present in this switch. A port can be mapped to any of the groups. Multiple ports can also be mapped to a group with same group Id.
Note: By default, each port is mapped to a group with a group Id equal to the port number. For example, port 1 is mapped to the group with ID=1.

Port Members

A row of radio buttons, one radio button for each port is displayed for each Group ID. To include a port in a Group, click the radio button. A port must belong to at least one group.

Adding a New Port to Group mapping entry

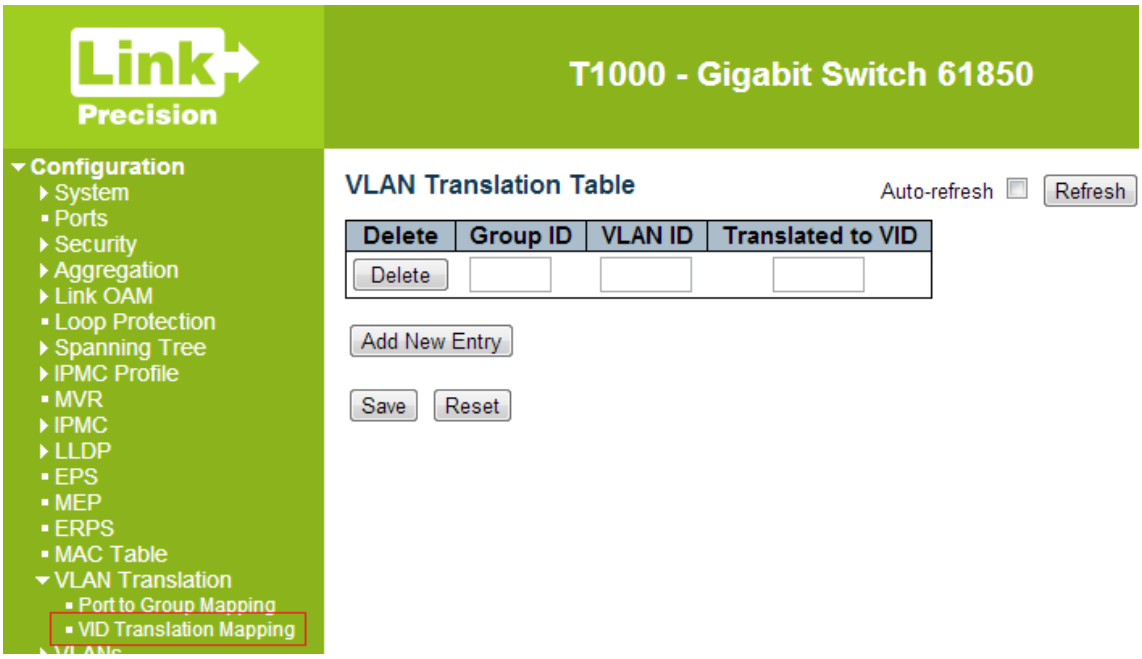
Click to add a new entry in Port to Group Mapping Table. An empty row is added to the table with the Group ID and array of radio buttons, one radio button for each port(click corresponding radio button to make port to be member of a particular Group). Note that if a VLAN translation is enabled on a management port for management VLAN, it may disrupt the management connectivity in some cases.

Legal values for a VLAN ID are 1 through 409.
The button can be used to undo the addition of new entry.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

VLAN Translation Mapping Table



This page allows you to map VLAN ID to other VLAN ID for a particular Group ID Globally.
The displayed settings are:

Delete

To delete a VLAN Translation Group database entry, check this box. The entry will be deleted on the switch during the next Save

Group ID

A valid Group ID is an integer value from 1 to 14. A set of VLAN Translations are mapped to a group Id. This way a port is mapped to a list of VLAN Translations easily by mapping it to a group. Number of groups in a switch is equal to the number of ports present in this switch. A port can be mapped to any of the groups. Multiple ports can also be mapped to a group with same group Id.
Note: By default, each port is mapped to a group with a group Id equal to the port number. For example, port 1 is mapped to the group with ID=1.

VLAN ID

Indicates the ID to which Group ID will be mapped. A valid VLAN ID ranges from 1-409.

Translated to VLAN ID

Indicates the VID to which VLAN ID of ingress frames will be changed, if VID in incoming frames if same as configured in VLAN ID field preceded by this field on member ports of a particular group to which this entry belongs.

Adding a New VLAN Translation entry

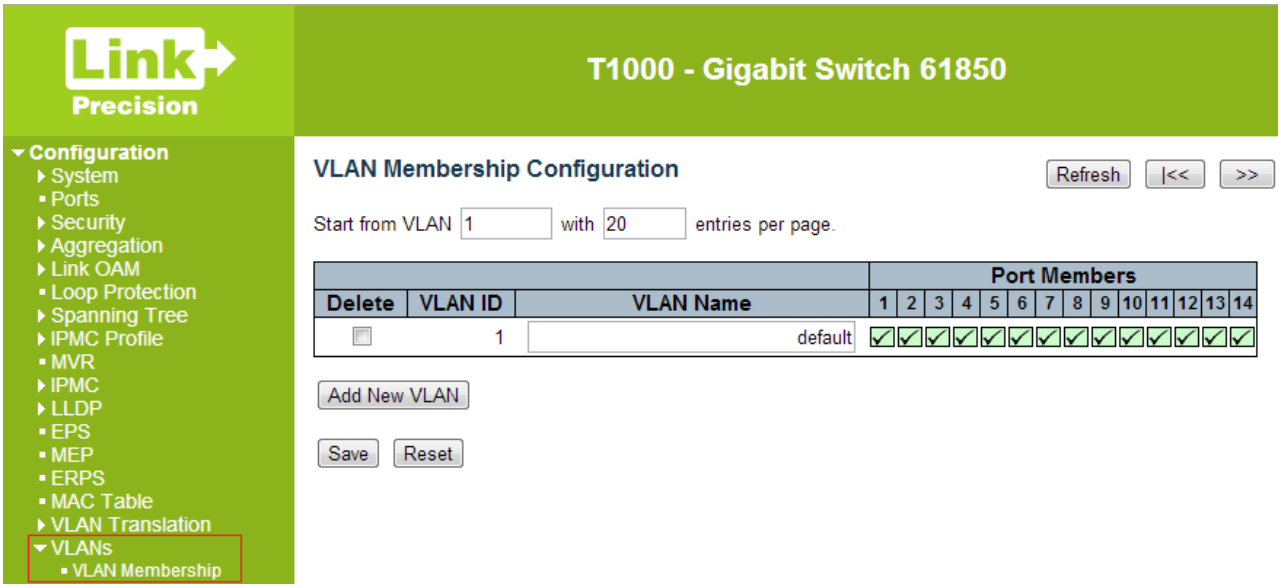
Click to add a new entry in VLAN Translation table. An empty row is added to the table, the Group ID, VLAN ID and Translated to VID fields can be configured as needed. Legal values for a VLAN ID are 1through 409.
The button can be used to undo the addition of new entry.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

VLAN

VLAN Membership Configuration



The VLAN membership configuration for the switch can be monitored and modified here. Up to 4096 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

Navigating the VLAN Table

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the closest next VLAN Table match. The will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

Delete

To delete a VLAN entry, check this box. The entry will be deleted during the next Save.

VLAN ID

Indicates the ID of this particular VLAN.

VLAN Name

Indicates the name of the VLAN. Maximum length of the VLAN Name String is 32. VLAN Name can be null. If it is not null, it must contain alphabets or numbers. At least one alphabet must be present in a non-null VLAN name. VLAN name can be edited for the existing VLAN entries or it can be added to the new entries.

Port Members

A row of check boxes for each port is displayed for each VLAN ID.
To include a port in a VLAN, check the box as .
To include a port in a forbidden port list, check the box as shown .
To remove or exclude the port from the VLAN, make sure the box is unchecked as shown .
By default, no ports are members, and for every new VLAN entry all boxes are unchecked.

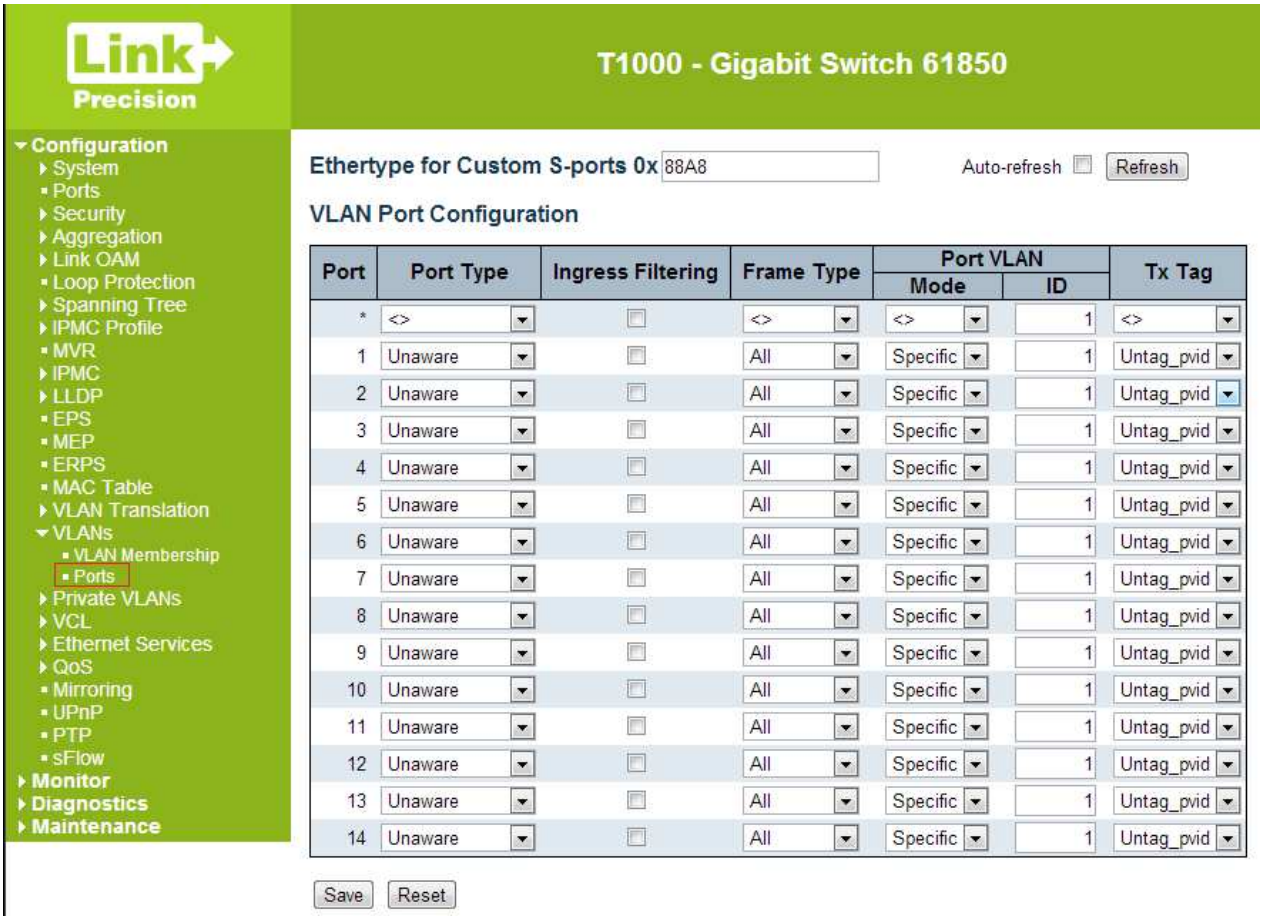
Adding a New VLAN

Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through409.
The VLAN is enabled when you click on "Save". The button can be used to undo the addition of new VLANs.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.
REFRESH: Refreshes the displayed table starting from the "VLAN ID" input fields.
|<<: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
>>: Updates the table, starting with the entry after the last entry currently displayed.

VLAN Port Configuration



This page is used for configuring the switch port VLAN.

Ethertype for Custom S-ports

This field specifies the ether type used for Custom S-ports. This is a global setting for all the Custom S-ports.

Port

This is the logical port number of this row.

Port Type

Port can be one of the following types: Unaware, Customer port(C-port), Service port(S-port), Custom Service port(S-custom-port)
If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.

Ingress Filtering

Enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).

Frame Type

Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.

Port VLAN Mode

Configures the Port VLAN Mode. The allowed values areNone or Specific. This parameter affects VLAN ingress and egress processing.
If None is selected, a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches. Tx tag should be set to Untag_pvid when this mode is used.
If Specific (the default value) is selected, a Port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.

Port VLAN ID

Configures the VLAN identifier for the port. The allowed values are from 1 through 409. The default value is1.
Note: The port must be a member of the same VLAN as the Port VLAN ID.

Tx Tag

Determines egress tagging of a port. Untag_pvid - All VLANs except the configured PVID will be tagged. Tag_all - All VLANs are tagged. Untag_all - All VLANs are untagged.

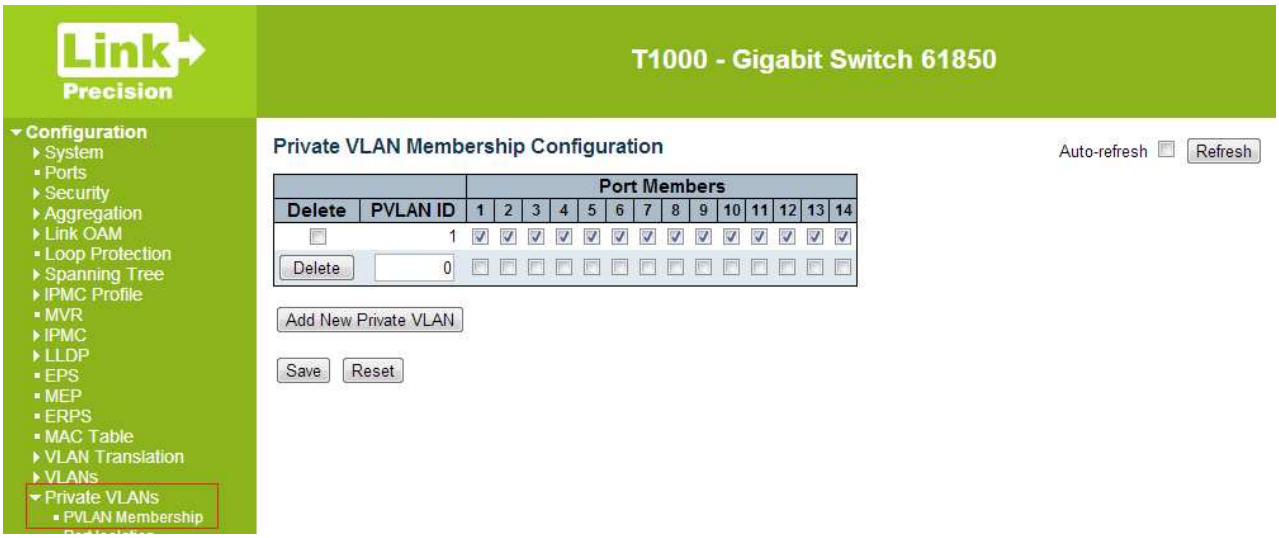
Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

Private VLAN

Private VLAN Membership Configuration

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or



removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Delete

To delete a private VLAN entry, check this box. The entry will be deleted during the next save.

Private VLAN ID

Indicates the ID of this particular private VLAN.

Port Members

A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

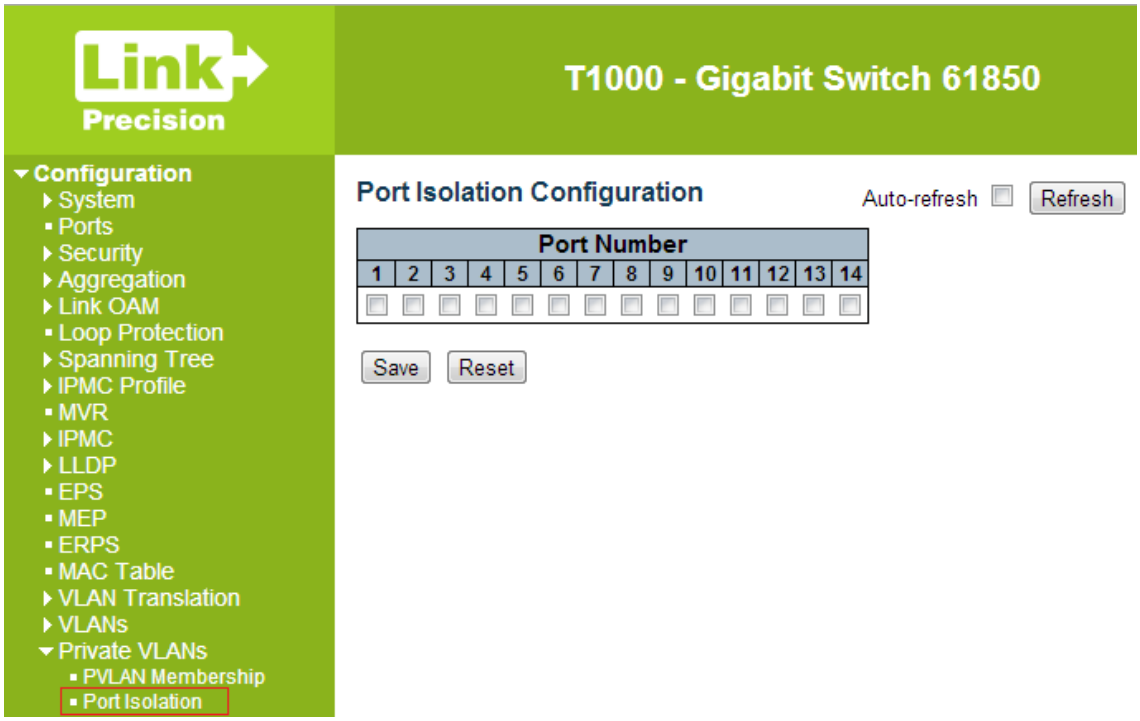
Adding a New Private VLAN

Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction.
The Private VLAN is enabled when you click "Save".
The button can be used to undo the addition of new Private VLANs.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFESH: Click to refresh the page immediately.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

Port Isolation Configuration



This page is used for enabling or disabling port isolation on ports in a Private VLAN.
A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Configuration

Port Members

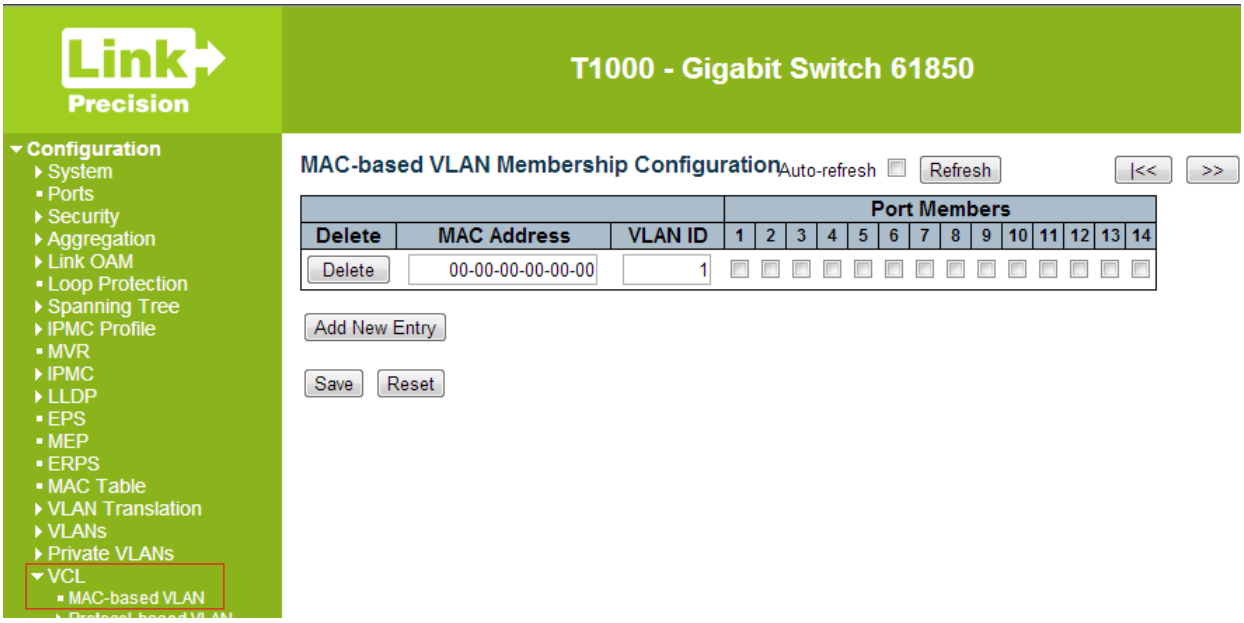
A check box is provided for each port of a private VLAN.
When checked, port isolation is enabled on that port.
When unchecked, port isolation is disabled on that port.
By default, port isolation is disabled on all ports.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

VCL

VCL MAC-Based VLAN Configuration



The MAC-based VLAN enties can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Delete

To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted in the stack.

MAC Address

Indicates the MAC address.

VLAN ID

Indicates the VLAN ID.

Port Members

A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New MAC-based VLAN

Click to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-

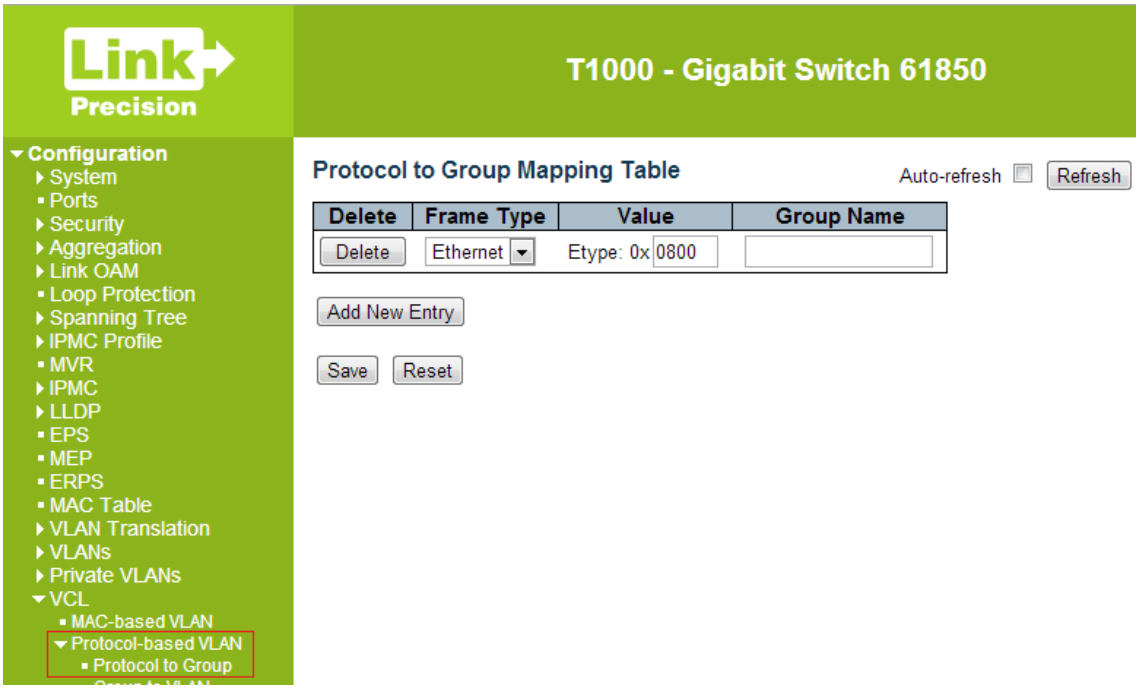
based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through409.
The MAC-based VLAN entry is enabled when you click on "Save". A MAC-based VLAN without any port members will be deleted when you click "Save".
The button can be used to undo the addition of new MAC-based VLANs. The maximum possible MAC-based VLAN entries are limited to 26.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Refreshes the displayed table.
|<<: Updates the table starting from the first entry in the MAC-based VLAN Table.
>>: Updates the table, starting with the entry after the last entry currently displayed.

Protocol-Based VLAN

Protocol to Group Mapping Table



This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the switch .
The displayed settings are:

Delete

To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.

Frame Type

Frame Type can have one of the following values:
1. Ethernet
2. LLC
3. SNAP

Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.

Value

Valid value that can be entered in this text field depends on the option selected from the the preceding Frame Type selection menu.
Below is the criteria for three different Frame Types:
1. For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff
2. For LLC: Valid value in this case is comprised of two different sub-values.
    a. DSAP: 1-byte long string (0x00-0xff)
    b. SSAP: 1-byte long string (0x00-0xff)
3. For SNAP: Valid value in this case also is comprised of two different sub-values.

a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.
b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.

In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

Group Name

A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9).
Note: special character and underscore(_) are not allowed.

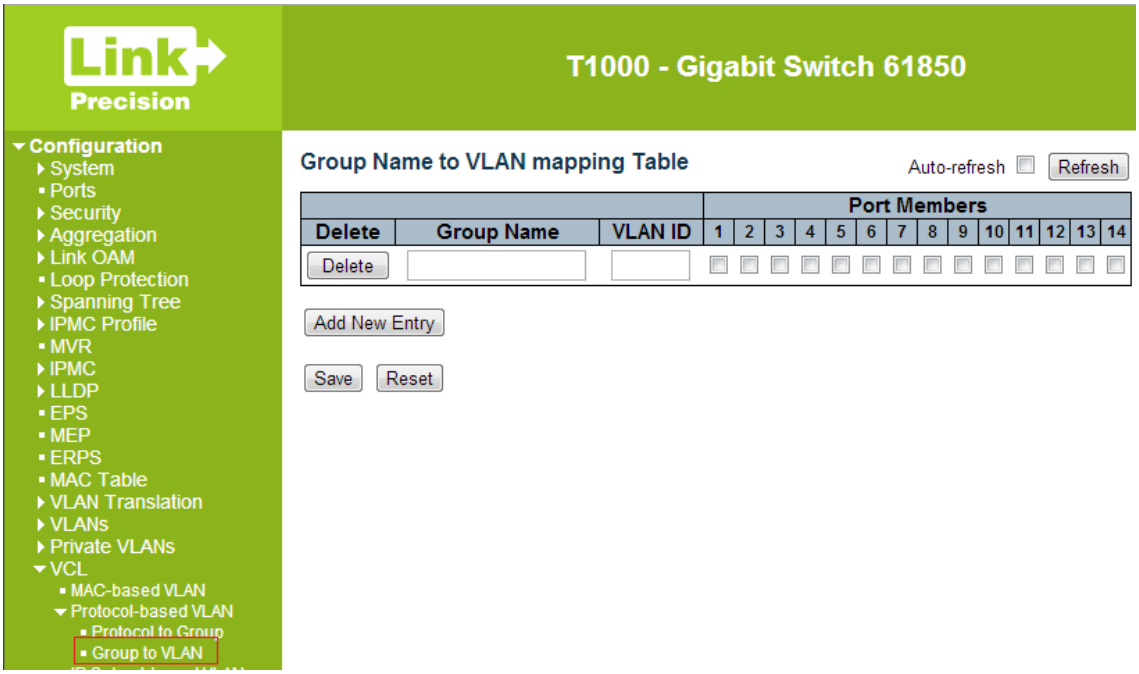
Adding a New Group to VLAN mapping entry

Click to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed.
The button can be used to undo the addition of new entry. The maximum possible Protocol to Group mappings are limited to 128.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.

Group Name to VLAN mapping Table



This page allows you to map a already configured Group Name to a VLAN for the switch .
The displayed settings are:

Delete

To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next
Save

Group Name

A valid Group Name is a string at the most 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be pre-used by any other existing mapping entry on this page.

VLAN ID

Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-409.

Port Members

A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New Group to VLAN mapping entry

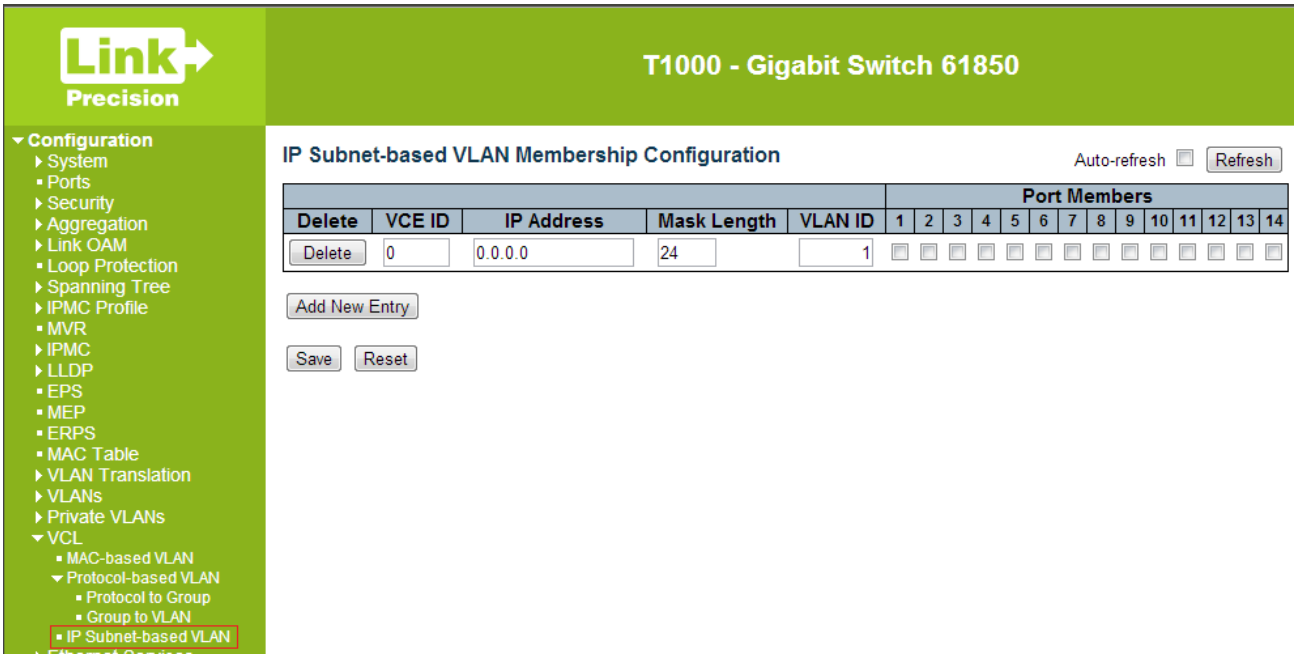
Click to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 409.
The button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 64.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

REFRESH: Click to refresh the page immediately.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

VCL IP Subnet-based VLAN Configuration



The IP subnet-based VLAN enties can be configured here. This page allows for adding, updating and deleting IP subnet-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Delete

To delete a IP subnet-based VLAN entry, check this box and press save. The entry will be deleted in the stack.

VCE ID

Indicates the index of the entry. It is user configurable. It's value ranges from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.

IP Address

Indicates the IP address.

Mask Length

Indicates the network mask length.

VLAN ID

Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

Port Members

A row of check boxes for each port is displayed for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New IP subnet-based VLAN

Click to add a new IP subnet-based VLAN entry. An empty row is added to the table, and the IP subnet-based VLAN entry can be configured as needed. Any IP address/mask can be configured for the IP subnet-based VLAN entry. Legal values for a VLAN ID are 1 through409.

The IP subnet-based VLAN entry is enabled when you click on "Save". The button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128.

Buttons

SAVE: Click to save changes.

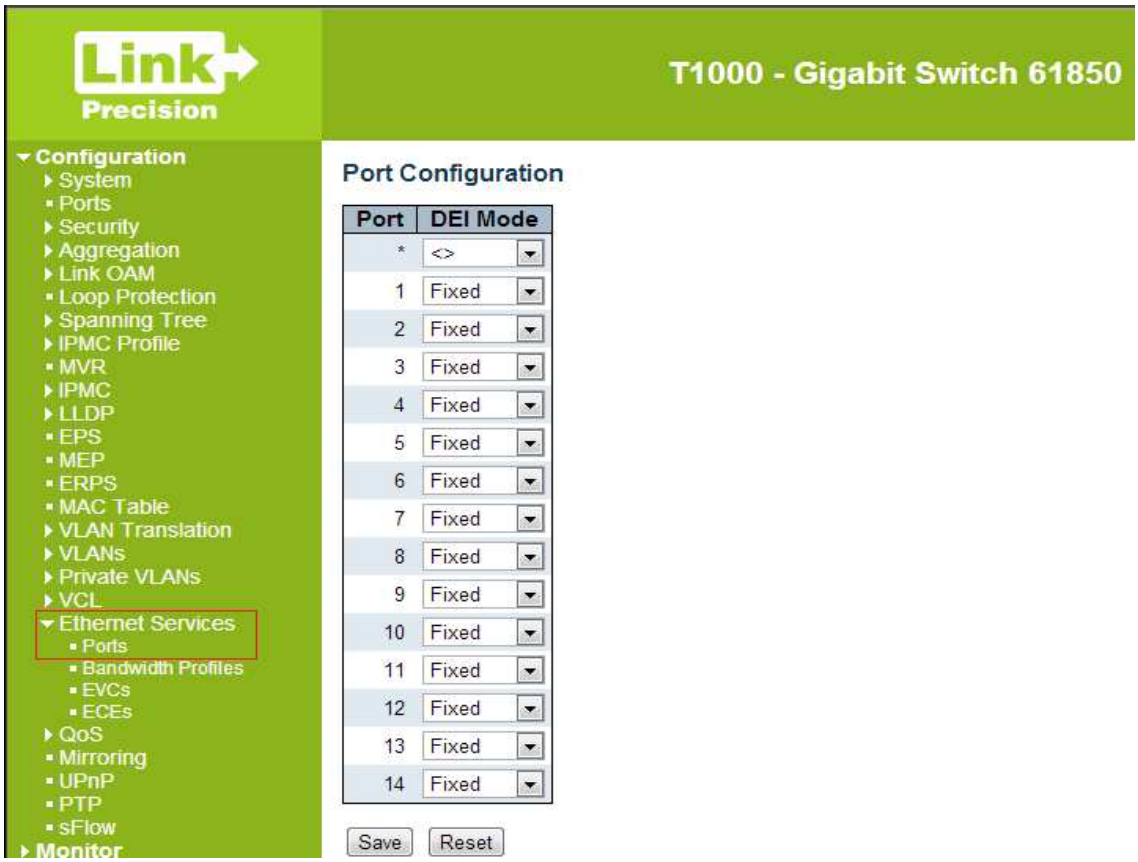
RESET: Click to undo any changes made locally and revert to previously saved values.

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

RESFRESH: Refreshes the displayed table.

Ethernet Services

EVC Port Configuration



This page displays current EVC port configurations. The settings can also be configured here.

Port

The logical port for the settings contained in the same row.

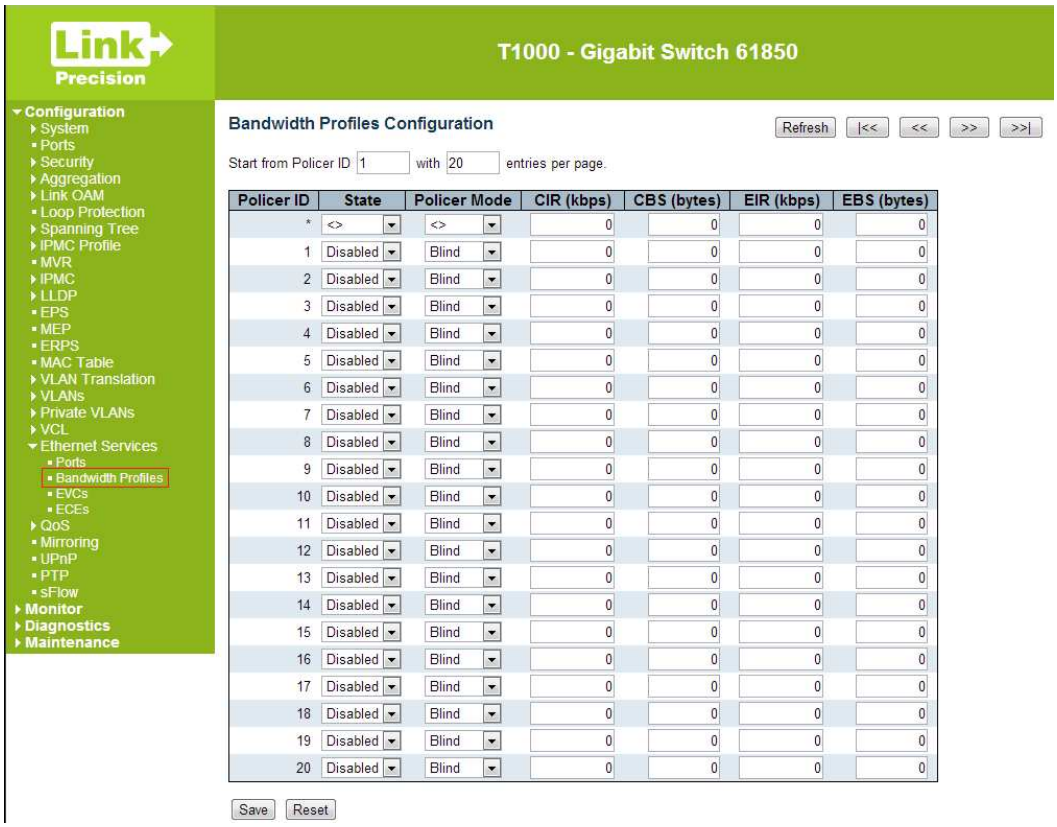
DEI Mode

The DEI mode for an NNI port determines whether frames transmitted on the port will have the DEI field in the outer tag marked based on the colour of the frame. The allowed values are:
Coloured: The DEI is 1 for yellow frames and 0 for green frames.
Fixed: The DEI value is determined by ECE rules.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

EVC Bandwidth Profile Configuration



This page displays current EVC ingress bandwidth profile configurations. These policers may be used to limit the traffic received on UNI ports. The settings can also be configured here.

Start Policer ID

The start Policer ID for displaying the table entries. The allowed range is from 1 through 2048.

Number of Entries

The number of entries per page. The allowed range is from2 through 2048.

Policer ID

The Policer ID is used to identify one of the 2048 policers.

State

The administrative state of the bandwidth profile. The allowed values are:
Enabled: The bandwidth profile enabled.
Disabled: The bandwidth profile is disabled.

Policer Mode

The colour mode of the bandwidth profile. The allowed values are:
Coupled: Colour-aware mode with coupling enabled.

Aware: Colour-aware mode with coupling disabled.
Blind: Colour-blind mode.

CIR

The Committed Information Rate of the bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.

CBS

The Committed Burst Size of the bandwidth profile. The allowed range is from 0 through 100000 bytes.

EIR

The Excess Information Rate of the bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.

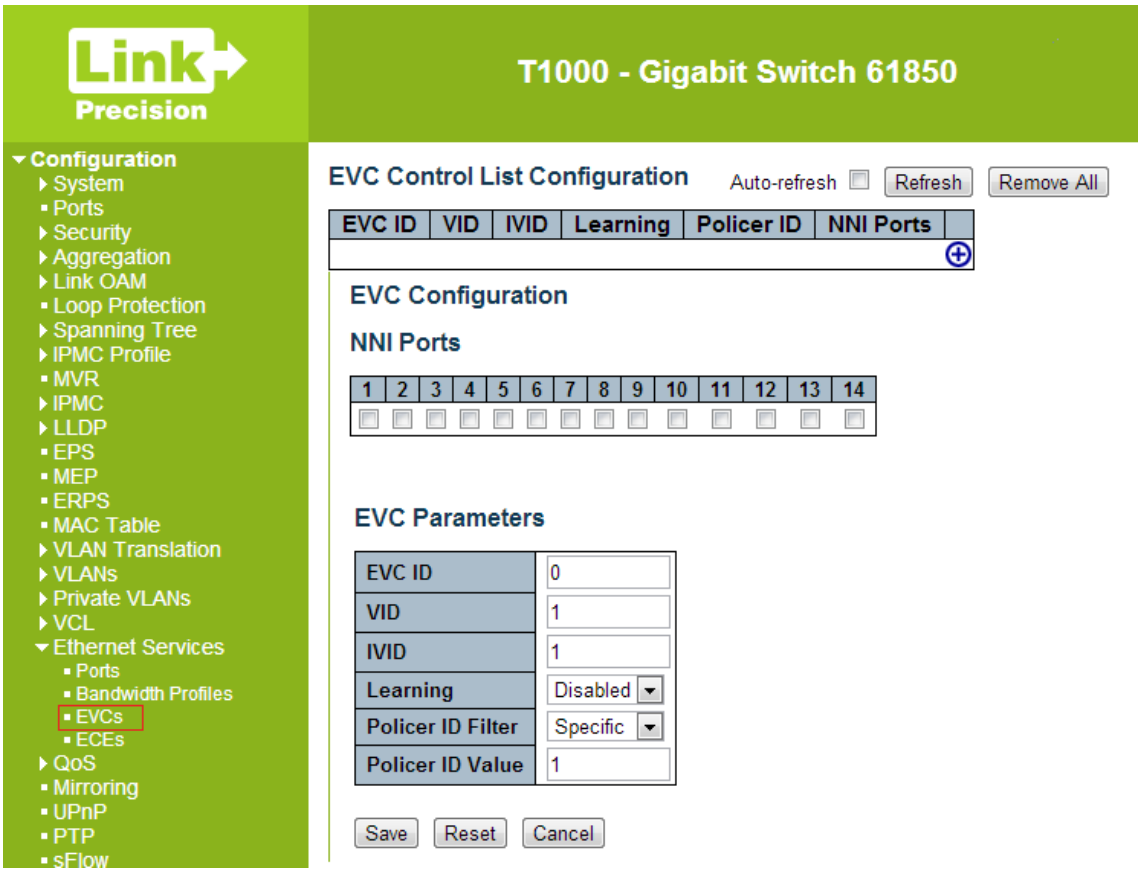
EBS

The Excess Burst Size of the bandwidth profile. The allowed range is from 0 through 100000 bytes.

Buttons

REFRESH: Refreshes the displayed table starting from the input fields.
|<<: Updates the table, starting with the first entry in the table.
<<: Updates the table, ending at the entry before the first entry currently displayed.
>>: Updates the table, starting with the entry after the last entry currently displayed.
>>|: Updates the table, ending at the last entry in the table.
SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

EVC Control List Configuration



This page displays current EVC configurations. On this system, only Provider Bridge based EVCs are supported.

EVC ID

The EVC ID identifies the EVC. The range is from 1through 128.

VID

The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLANconfiguration. The range is from 1 through 409.

IVID

The Internal/classified VLAN ID in the PB network. The range is from 1 through 409.

Learning

The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. The possible values are:
Enabled: Learning is enabled (MAC addresses are learned).
Disabled: Learning is disabled (MAC addresses are not learned).

Policer ID

The ingress bandwidth profile mode for the EVC. The possible values are:

Specific: The range is from 1 through 128.
Discard: All received frames are discarded for the EVC.
None: None bandwidth profile for the EVC.

NNI Ports

The list of Network to Network Interfaces for the EVC.

Modification Buttons

You can modify each EVC in the table using the following buttons:

: Edits the EVC row.

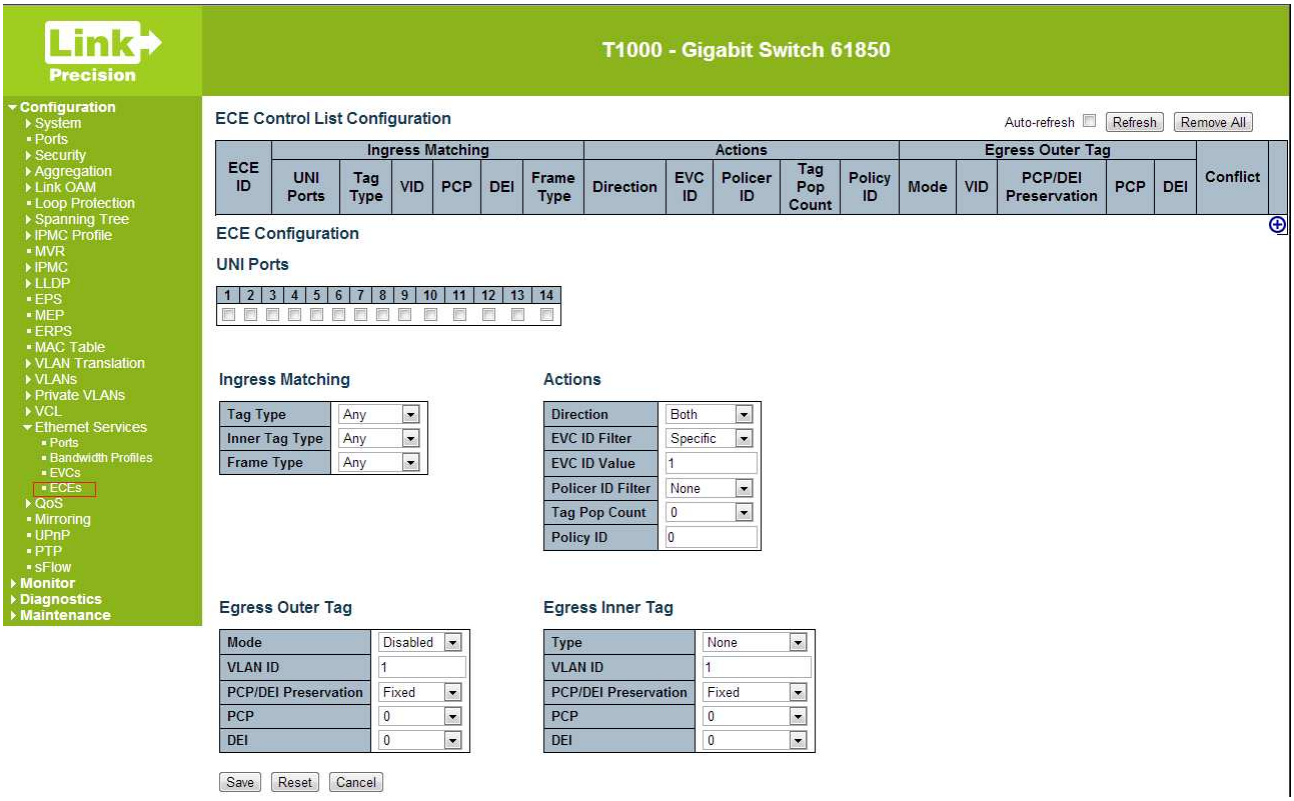
: Deletes the EVC.

: Adds new EVC.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page.
REMOVE ALL: Click to remove all EVCs.

ECE Configuration



This page displays current ECE configurations. The settings can also be configured here.

UNI Ports

The list of User Network Interfaces for the ECE.

UNI Matching

Tag Type

The tag type for matacching the ECE. The possible values are:
Any: The ECE will match both tagged and untagged frames.
Untagged: The ECE will match untagged frames only.
C-Tagged: The ECE will match coustom tagged frames only.
S-Tagged: The ECE will match service tagged frames only.
Tagged: The ECE will match tagged frames only.

VLAN ID Filter

The VLAN ID filter for matching the ECE. It only significant if tag type 'Tagged' is selected. The possible values are:
Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)
Specific: If you want to filter a specific VLAN ID value with this ECE, choose this value. A field for entering a specific value appears.
Range: If you want to filter a specific VLAN ID range filter with this ECE, choose this value. A field for entering a range appears.

VLAN ID Value

When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 0through 409.

VLAN ID Range
When "Range" is selected for the VLAN ID filter, you can enter a specific range. The allowed range is from 0through 409.

PCP
The PCP value for matching the ECE. It only significant if tag type 'Tagged' is selected. The possible values are:
Any: The ECE will match any PCP value.
Specific: The ECE will match a specific PCP in the range 0 through 7.
Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-, 6-7, 0-3 or 4-7.

DEI
The DEI value for matching the ECE. It only significant if tag type 'Tagged' is selected. The allowed value is: 0, 1 orAny.

Inner Tag Type
The inner tag type for matching the ECE. The possible values are:
Any: The ECE will match both tagged and untagged frames.
Tagged: The ECE will match tagged frames only.
C-Tagged: The ECE will match coustom tagged frames only.
S-Tagged: The ECE will match service tagged frames only.
Untagged: The ECE will match untagged frames only.

Inner VLAN ID Filter
The inner VLAN ID filter for matching the ECE. It only significant if tag type 'Tagged' is selected. The possible values are:
Any: No inner VLAN ID filter is specified. (Inner VLAN ID filter status is "don't-care".)
Specific: If you want to filter a specific inner VLAN ID value with this ECE, choose this value. A field for entering a specific value appears.
Range: If you want to filter a specific inner VLAN ID range filter with this ECE, choose this value. A field for entering a range appears.

Inner VLAN ID Value
When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 0through 409.

Inner VLAN ID Range
When "Range" is selected for the VLAN ID filter, you can enter a specific range. The allowed range is from 0through 409.

Inner Tag PCP
The inner PCP value for matching the ECE. It only significant if inner tag type 'Tagged' is selected. The possible values are:
Any: The ECE will match any PCP value.
Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-, 6-7, 0-3 or 4-7.
Specific: The ECE will match a specific PCP in the range 0 through 7.

Inner Tag DEI
The inner DEI value for matching the ECE. It only significant if inner tag type 'Tagged' is selected. The allowed value is: 0, 1 or Any.

Frame Type

The frame type for the ECE. The possible values are:
Any: The ECE will match any frame type.
IPv4: The ECE will match IPv4 frames only.
IPv6: The ECE will match IPv6 frames only.

DSCP Filter
The DSCP filter for matching the ECE. The possible values are:
Any: No DSCP filter is specified. (DSCP filter status is "don't-care".)
Specific: If you want to filter a specific DSCP value with this ECE, choose this value. A field for entering a specific value appears.
Range: If you want to filter a specific DSCP range filter with this ECE, choose this value. A field for entering a range appears.

DSCP Value
When "Specific" is selected for the DSCP filter, you can enter a specific value. The allowed value is from 0through 63.

DSCP Range
When "Range" is selected for the DSCP filter, you can enter a specific range. The allowed range is from 0 through63.

Actions

Direction
The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. The possible values are:
Both: Bidirectional.
UNI-to-NNI: Unidirectional from UNI to NNI.
NNI-to-UNI: Unidirectional from NNI to UNI.

EVC ID Filter
The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. The possible values are:
Any: No EVC ID filter is specified. (EVC ID filter status is "don't-care".)
Specific: If you want to filter a specific EVC ID with this ECE, choose this value. A field for entering a specific value appears.

EVC ID Value
When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 1through 4096.

Policer ID Filter
The policer ID filter for matching the ECE. The possible values are:
Specific: If you want to filter a specific policer ID value with this ECE, choose this value. A field for entering a specific value appears.
Discard: All received frames are discarded for the ECE.
None: All received frames are forwarded for the ECE.
None:The bandwidth profile for the specified EVC ID is used.

Policer ID Value
When "Specific" is selected for the policer ID filter, you can enter a specific value. The value is from 1 through2048.

Tag Pop Count
The ingress tag pop count for the ECE. The allowed range is from 0 through 2.

Policy ID
The ACL Policy ID for the ECE for matching ACL rules. The allowed range is from 0 through 2.

Egress Outer Tag

Outer Tag Mode
The outer tag for nni-to-uni direction for the ECE. The possible values are:
Enable: Enable outer tag for nni-to-uni direction for the ECE.
Disable: Disable outer tag for nni-to-uni direction for the ECE.

Outer Tag VID
The EVC outer tag VID for UNI ports. The allowed value is from 0 through 409.

Outer Tag PCP/DEI Preservation
The outer tag PCP and DEI preservation for the ECE. The possible values are:
Preserved: The outer tag PCP and DEI is preserved.
Fixed: The outer tag PCP and DEI is fixed.

Outer Tag PCP
The outer tag PCP value for the ECE. The allowed range is from 0 through 7.

Outer Tag DEI
The outer tag DEI value for the ECE. The allowed value is0 or 1.

Egress Inner Tag

Inner Tag Type
The inner type for the ECE determines whether an inner tag is inserted in frames forwarded to NNI ports. The possible values are:
None: An inner tag is not inserted.
C-tag: An inner C-tag is inserted.
S-tag: An inner S-tag is inserted.
S-custom-tag: An inner tag is inserted and the tag type is determined by the VLAN port configuration of the NNI.

Inner Tag VLAN ID
The inner tag VLAN ID for the ECE. The allowed range is from 0 through 409.

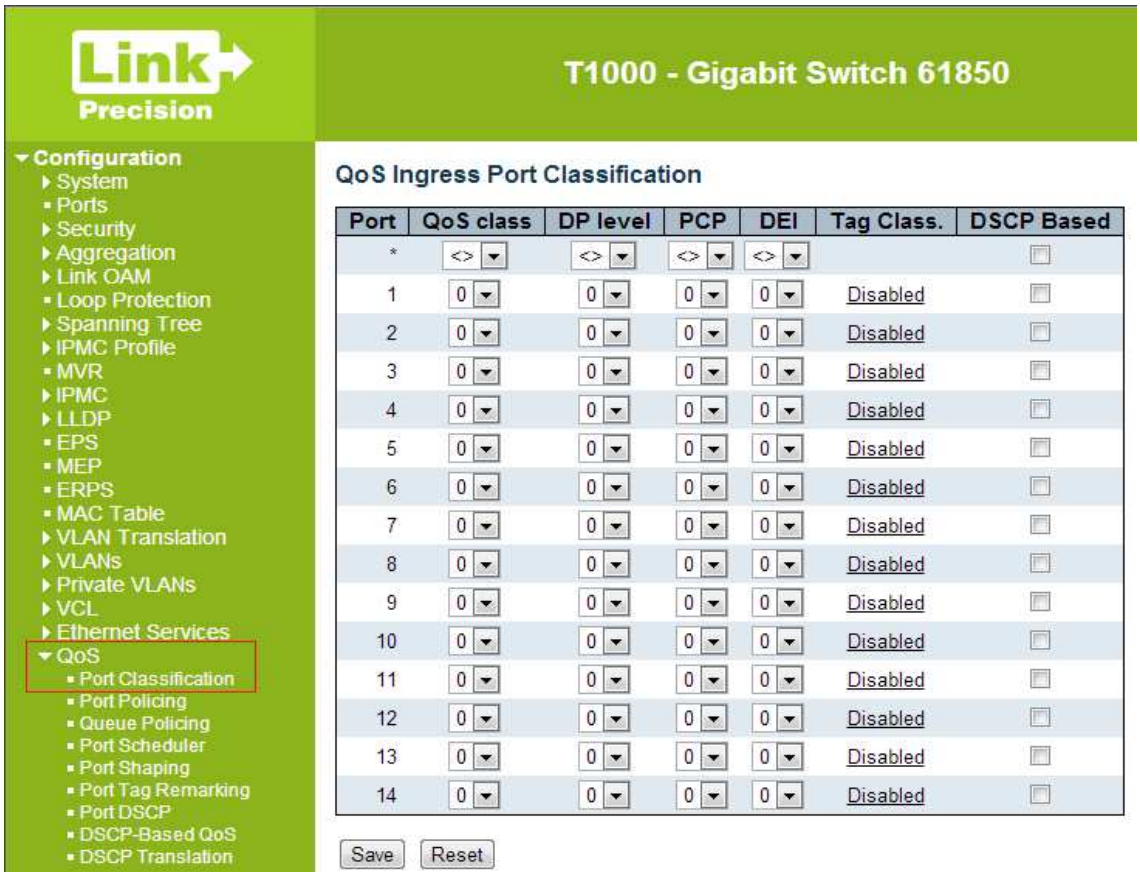
Inner Tag PCP Mode
The inner tag PCP mode for the ECE. The possible values are:
Classified: The inner tag PCP Mode is classified.
Fixed: The inner tag PCP Mode is classified.
Mapped: The inner tag PCP Mode is based on mapped (QOS, DP).

Inner Tag PCP
The inner tag PCP value for the ECE. The allowed range is from 0 through 7.

Inner Tag DEI
The inner tag DEI value for the ECE. The allowed value is0 or 1.

QoS

QoS Ingress Port Classification



This page allows you to configure the basic QoS Ingress Classification settings for all switch ports.
The displayed settings are:

Port

The port number for which the configuration below applies.

QoS class

Controls the default QoS class.
All frames are classified to a QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.
If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a QoS class that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default QoS class.
The classified QoS class can be overruled by a QCL entry.

Note: If the default QoS class has been dynamically changed, then the actual default QoS class is shown in parentheses after the configured default QoS class.

DP level

Controls the default Drop Precedence Level.
All frames are classified to a DP level.
If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DP level that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DP level.
The classified DP level can be overruled by a QCL entry.

PCP

Controls the default PCP value.
All frames are classified to a PCP value.
If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.

DEI

Controls the default DEI value.
All frames are classified to a DEI value.
If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.

Tag Class

Shows the classification mode for tagged frames on this port.
Disabled: Use default QoS class and DP level for tagged frames.
Enabled: Use mapped versions of PCP and DEI for tagged frames.
Click on the mode in order to configure the mode and/or mapping.
Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default QoS class and DP level.

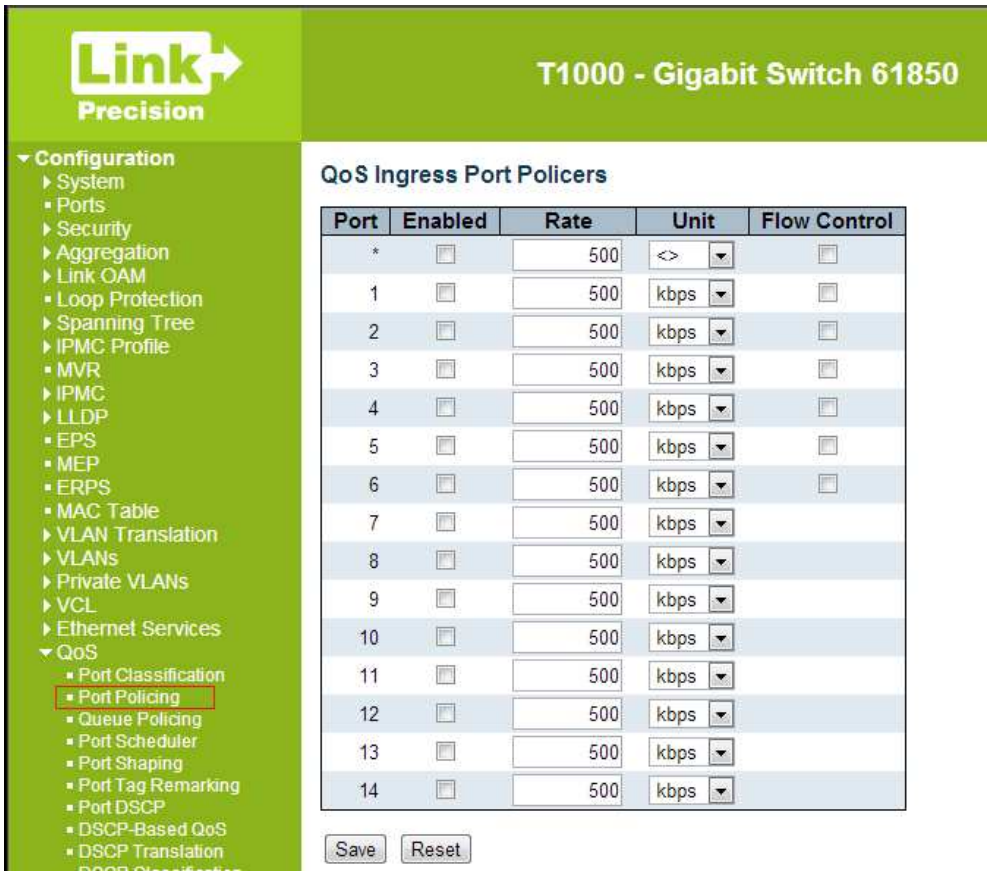
DSCP Based

Click to Enable DSCP Based QoS Ingress Port Classification.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

QoS Ingress Port Policing Configuration



This page allows you to configure the Policer settings for all switch ports.
The displayed settings are:

Port

The port number for which the configuration below applies.

Enabled

Controls whether the policer is enabled on this switch port.

Rate

Controls the rate for the policer. The default value is 00. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-13200 when the "Unit" is "Mbps" or "kfps".

Unit

Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".

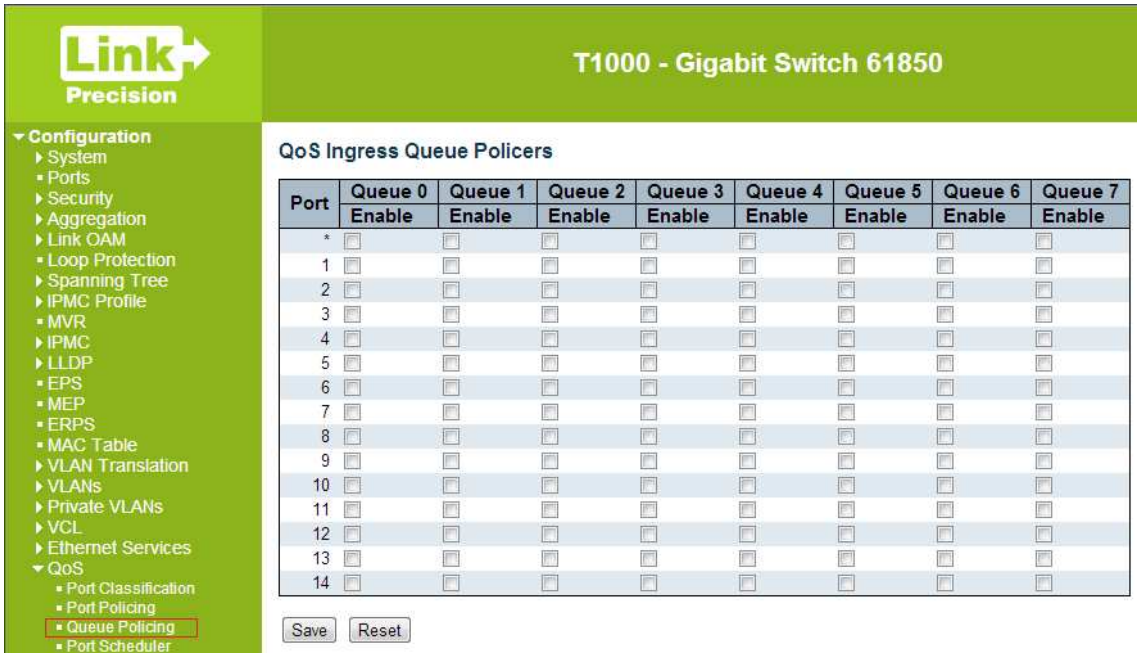
Flow Control

If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

QoS Ingress Queue Policing Configuration



This page allows you to configure the Queue Policer settings for all switch ports.
The displayed settings are:

Port

The port number for which the configuration below applies.

Enabled (E)

Controls whether the queue policer is enabled on this switch port.

Rate

Controls the rate for the queue policer. The default value is00. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".
This field is only shown if at least one of the queue policers are enabled.

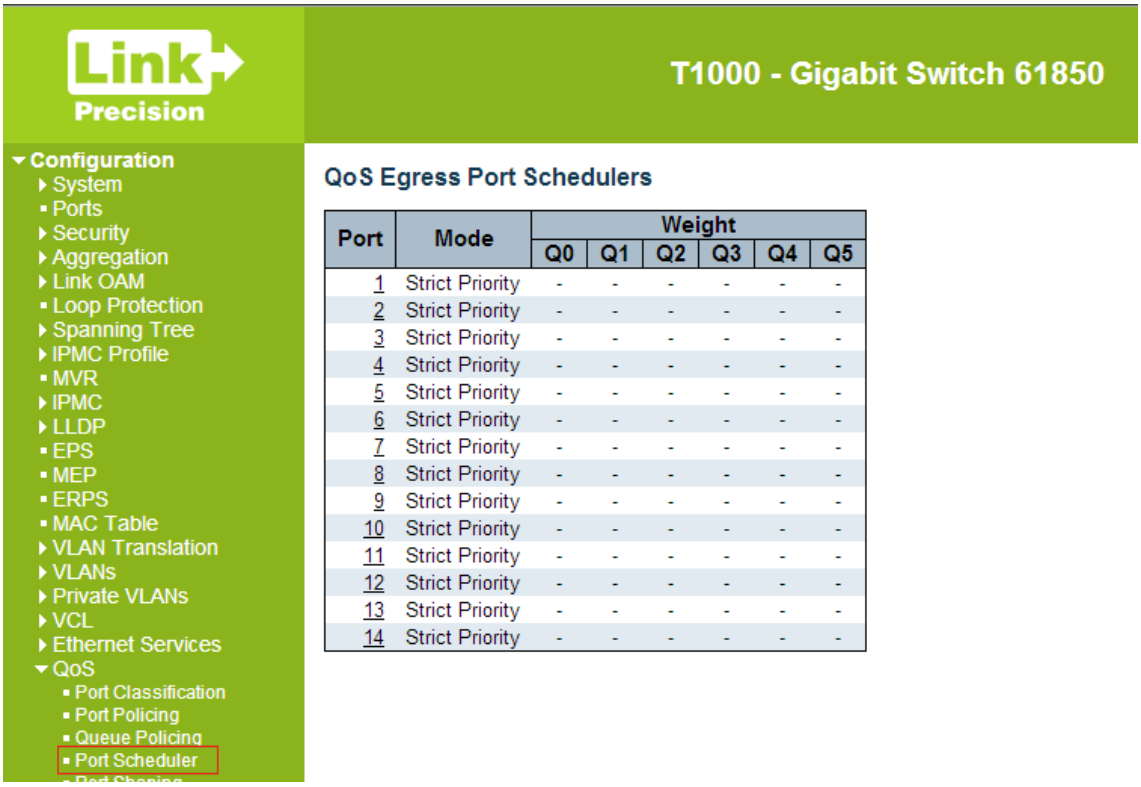
Unit

Controls the unit of measure for the queue policer rate as kbps or Mbps. The default value is "kbps".
This field is only shown if at least one of the queue policers are enabled.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

QoS Egress Port Schedulers



This page provides an overview of QoS Egress Port Schedulers for all switch ports.
The displayed settings are:

Port

The logical port for the settings contained in the same row.
Click on the port number in order to configure the schedulers.

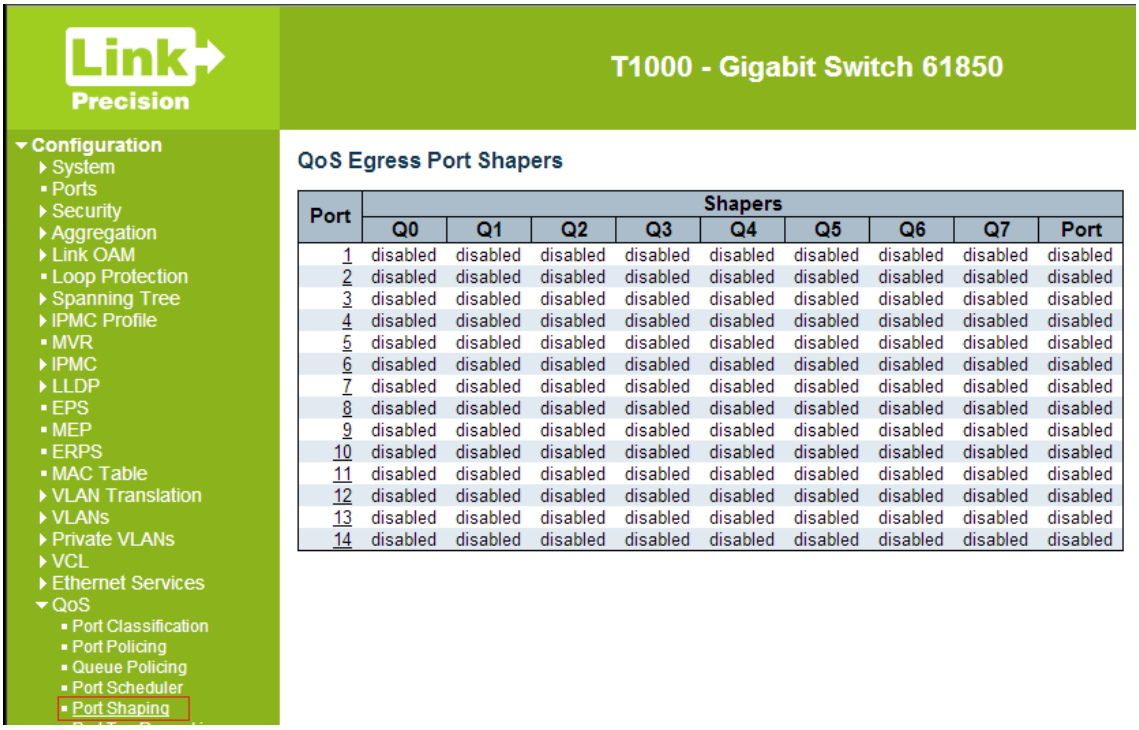
Mode

Shows the scheduling mode for this port.

Qn

Shows the weight for this queue and port.

QoS Egress Port Shapers


Link Precision
T1000 - Gigabit Switch 61850
Configuration
System
Ports
Security
Aggregation
Link OAM
Loop Protection
Spanning Tree
IPMC Profile
MVR
IPMC
LLDP
EPS
MEP
ERPS
MAC Table
VLAN Translation
VLANs
Private VLANs
VCL
Ethernet Services
QoS
Port Classification
Port Policing
Queue Policing
Port Scheduler
Port Shaping
QoS Egress Port Shapers
Port
Shapers
Q0 Q1 Q2 Q3 Q4 Q5 Q6 Q7 Port
1 disabled disabled disabled disabled disabled disabled disabled disabled disabled
2 disabled disabled disabled disabled disabled disabled disabled disabled disabled
3 disabled disabled disabled disabled disabled disabled disabled disabled disabled
4 disabled disabled disabled disabled disabled disabled disabled disabled disabled
5 disabled disabled disabled disabled disabled disabled disabled disabled disabled
6 disabled disabled disabled disabled disabled disabled disabled disabled disabled
7 disabled disabled disabled disabled disabled disabled disabled disabled disabled
8 disabled disabled disabled disabled disabled disabled disabled disabled disabled
9 disabled disabled disabled disabled disabled disabled disabled disabled disabled
10 disabled disabled disabled disabled disabled disabled disabled disabled disabled
11 disabled disabled disabled disabled disabled disabled disabled disabled disabled
12 disabled disabled disabled disabled disabled disabled disabled disabled disabled
13 disabled disabled disabled disabled disabled disabled disabled disabled disabled
14 disabled disabled disabled disabled disabled disabled disabled disabled disabled

This page provides an overview of QoS Egress Port Shapers for all switch ports.
The displayed settings are:

Port

The logical port for the settings contained in the same row.
Click on the port number in order to configure the shapers.

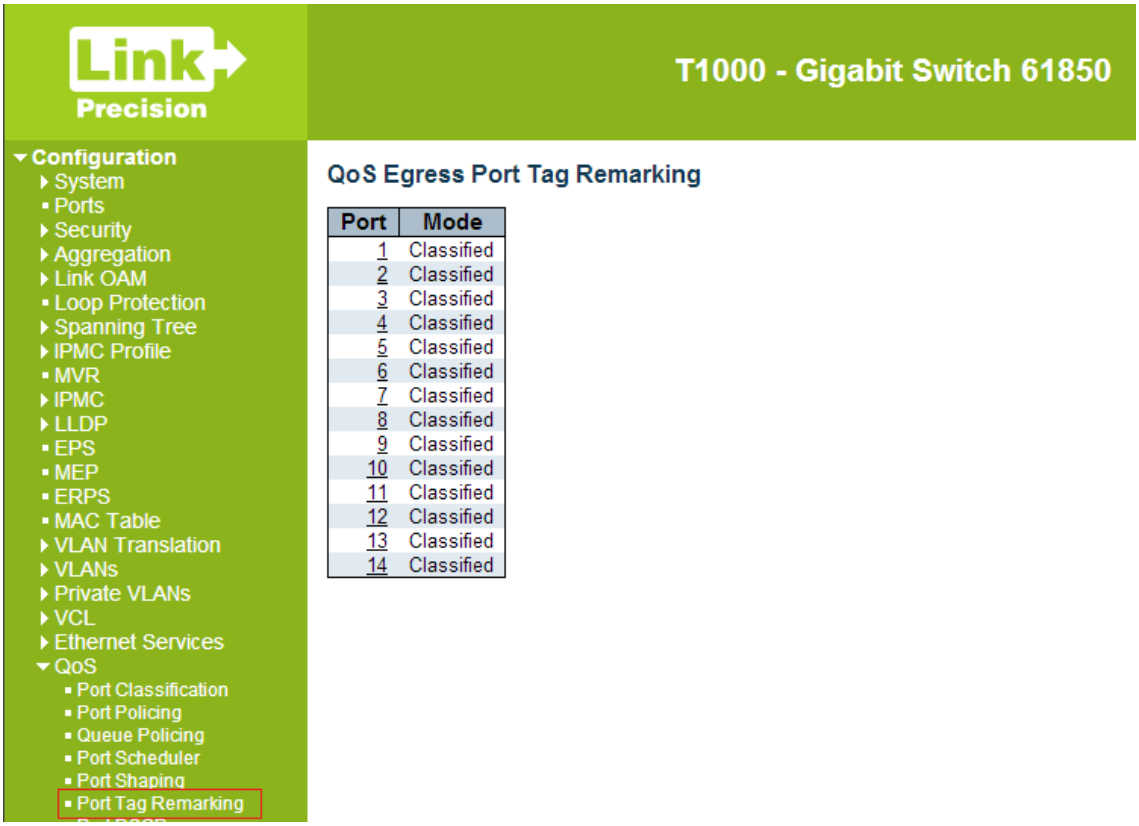
Qn

Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".

Port

Shows "disabled" or actual port shaper rate - e.g. "800 Mbps".

QoS Egress Port Tag Remarking



This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.
The displayed settings are:

Port

The logical port for the settings contained in the same row.
Click on the port number in order to configure tag remarking.

Mode

Shows the tag remarking mode for this port.
Classified: Use classified PCP/DEI values.
Default: Use default PCP/DEI values.
Mapped: Use mapped versions of QoS class and DP level.

Port DSCP Configuration

This page allows you to configure the basic QoS Port DSCPConfiguration settings for all switch ports. The displayed settings are:

Port

The Port column shows the list of ports for which you can configure dscp ingress and egress settings.

Ingress

In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress:

1. Translate
2. Classify

1. Translate

To Enable the Ingress Translation click the checkbox.

2. Classify

Classification for a port have 4 different values.

- Disable: No Ingress DSCP Classification.
- DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.
- Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.

• All: Classify all DSCP.

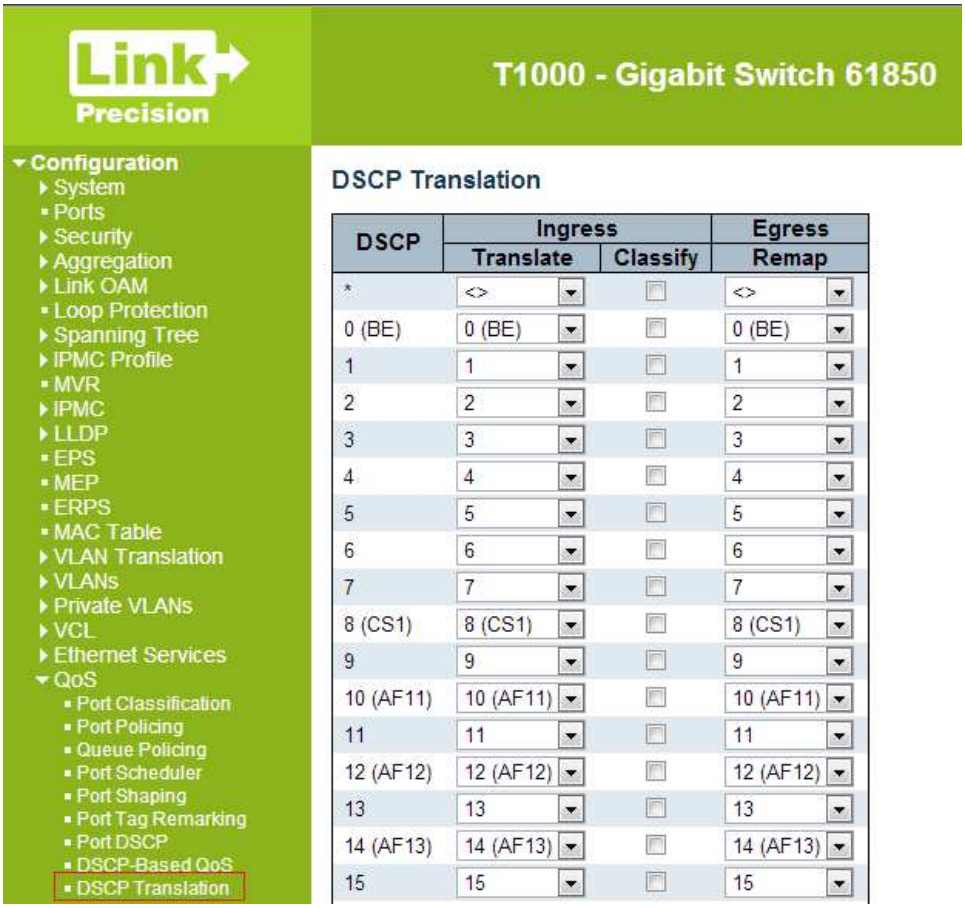
Egress

Port Egress Rewriting can be one of -
• Disable: No Egress rewrite.
• Enable: Rewrite enabled without remapping.
• Remap: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

DSCP Translation



This page allows you to configure the basic QoS DSCPTranslation settings for all switches. DSCP translation can be done in Ingress or Egress.
The displayed settings are:

DSCP

Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

Ingress

Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.
There are two configuration parameters for DSCP Translation -
1. Translate
2. Classify

1. Translate

DSCP at Ingress side can be translated to any of (0-63) DSCP values.

2. Classify

Click to enable Classification at Ingress side.

Egress

There is the following configurable parameter for Egress side –
· Remap

Remap

Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

DSCP Classification

This page allows you to configure the mapping of QoS class toDSCP value.
The displayed settings are:

QoS Class

Actual QoS class.

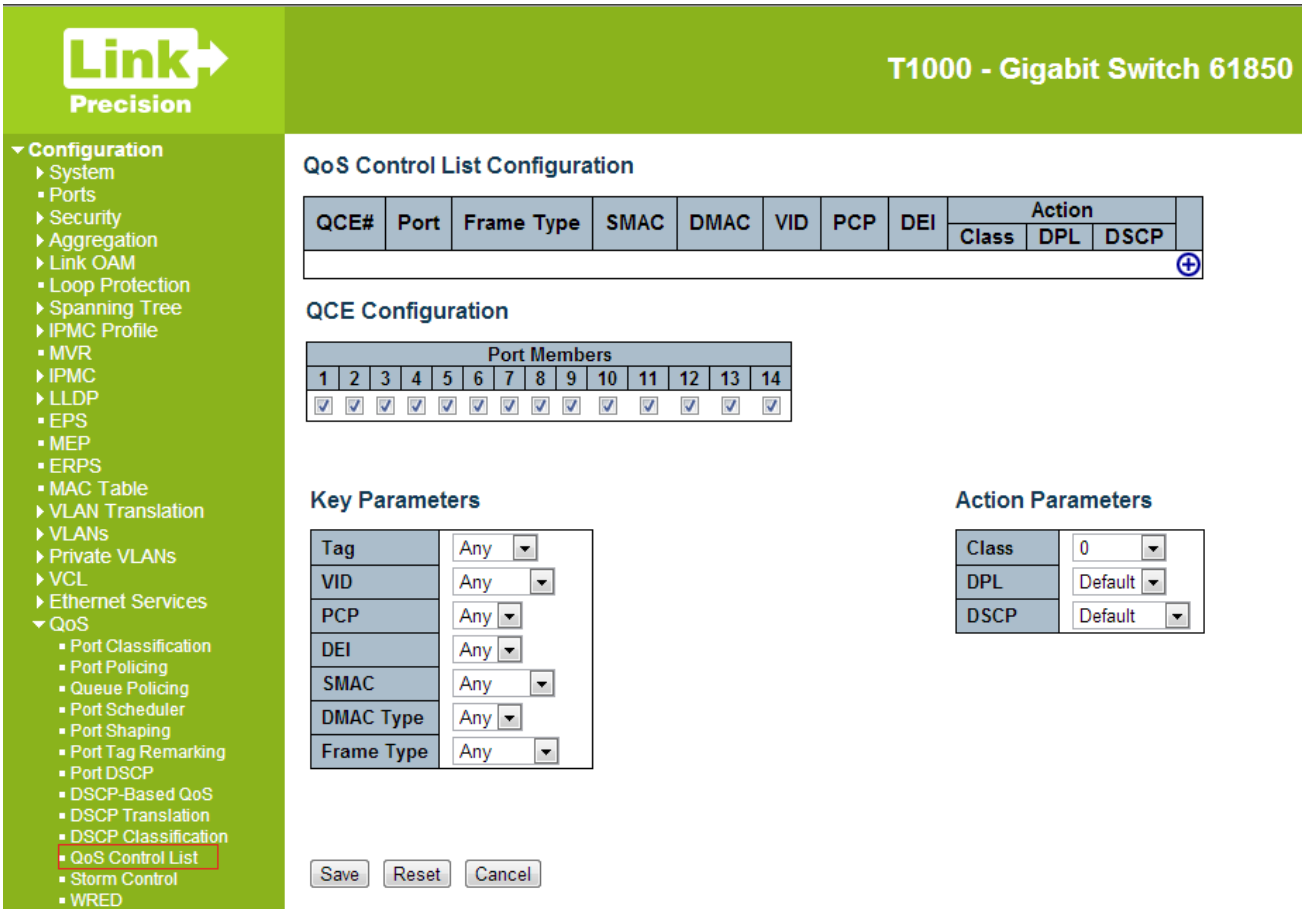
DSCP

Select the classified DSCP value (0-63).

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

QoS Control List Configuration



This page allows to edit|insert a single QoS Control Entry at a time. A QCE consists of several parameters. These parameters vary according to the frame type that you select.

Port Members

Check the checkbox button to include the port in the QCL entry. By default all ports are included.

Key Parameters

Key configuration is described as below:
Tag Value of Tag field can be 'Any', 'Untag' or 'Tag'.
VID Valid value of VLAN ID can be any value in the range 1-409 or 'Any'; user can enter either a specific value or a range of VIDs.
PCP Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, , 6, 7) or range(0-1, 2-3, 4-, 6-7, 0-3, 4-7) or 'Any'.
DEI Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.
SMAC Source MAC address: xx-xx-xx (24 MS bits OUI) or 'Any'.
DMAC Type Destination MAC type: possible values are unicast(UC), multicast(MC), broadcast(BC) or 'Any'.
Frame Type Frame Type can have any of the following values:
1. Any
2. Ethernet
3. LLC
4. SNAP
. IPv4

6. IPv6
Note: All frame types are explained below.

1. Any
Allow all types of frames.

2. Ethernet
Ethernet Type Valid ethernet type can have a value within 0x600-0xFFFF or 'Any' but excluding 0x800(IPv4) and 0x86DD(IPv6), default value is 'Any'.

3. LLC
SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'.
DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'.
Control Valid Control field can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'.

4. SNAP
PID Valid PID(a.k.a ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is 'Any'.

. IPv4
Protocol IP protocol number: (0-2, TCP or UDP) or 'Any'.
Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 2. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.
DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
IP Fragment IPv4 frame fragmented option: yes|no|any.
Sport Source TCP/UDP port:(0-63) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
Dport Destination TCP/UDP port:(0-63) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

6. IPv6
Protocol IP protocol number: (0-2, TCP or UDP) or 'Any'.
Source IP 32 LS bits of IPv6 source address in value/mask format or 'Any'.
DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
Sport Source TCP/UDP port:(0-63) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
Dport Destination TCP/UDP port:(0-63) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Action Parameters
Class QoS class: (0-7) or 'Default'.
DP Valid Drop Precedence Level can be (0-3) or 'Default'.
DSCP Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.
'Default' means that the default classified value is not modified by this QCE.

Buttons
SAVE: Click to save the configuration and move to main QCL page.
RESET: Click to undo any changes made locally and revert to previously saved values.
CANCEL: Return to the previous page without saving the configuration change.

Storm Control Configuration

This page allows you to configure the storm control settings for all switch ports.
There is a storm rate control for unicast frames, broadcast frames and unknown (flooded) frames.
The displayed settings are:

Port

The port number for which the configuration below applies.

Enabled

Controls whether the storm control is enabled on this switch port.

Rate

Controls the rate for the storm control. The default value is00. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-13200 when the "Unit" is "Mbps" or "kfps".

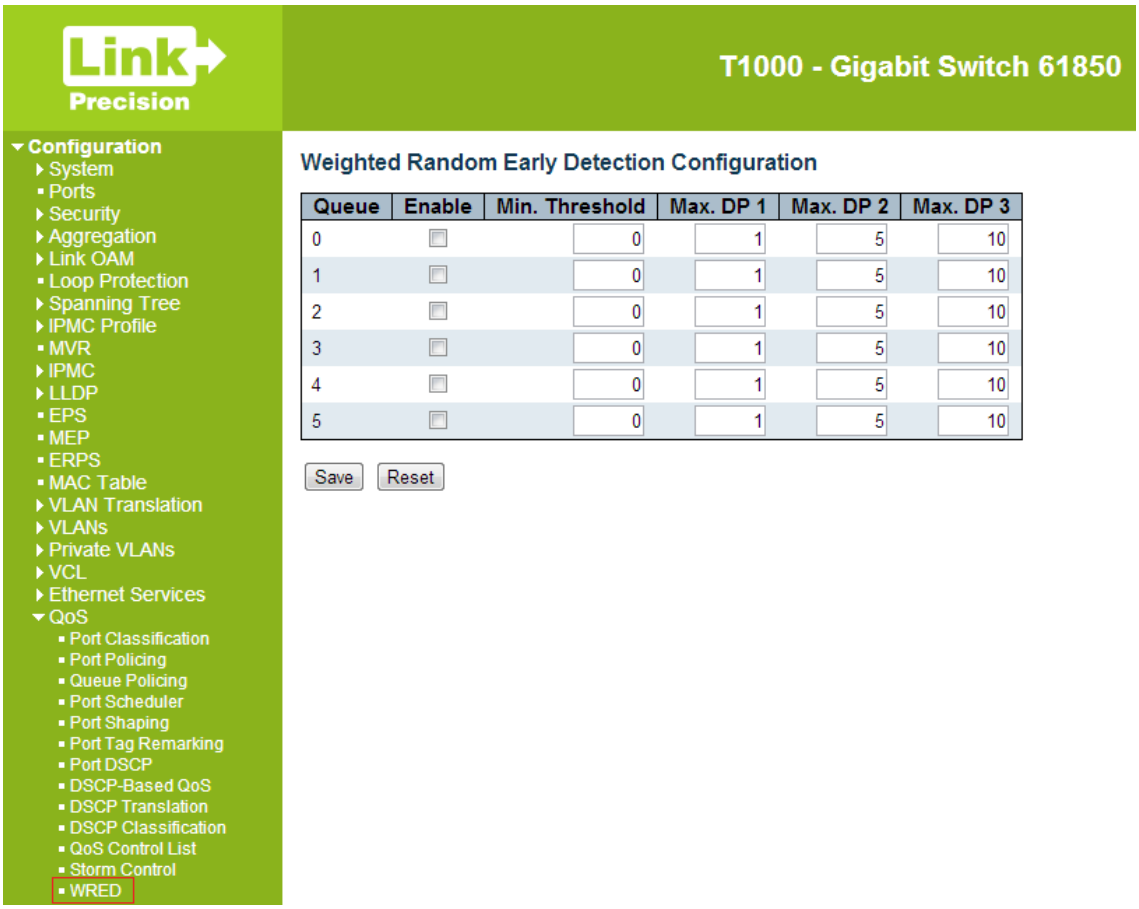
Unit

Controls the unit of measure for the storm control rate as kbps, Mbps, fps or kfps . The default value is "kbps".

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

QoS Weighted Random Early Detection



This page allows you to configure the Random Early Detection (RED) settings for queue 0 to .
RED cannot be applied to queue 6 and 7.
Through different RED configuration for the queues (QoS classes) it is possible to obtain Weighted Random Early
Detection (WRED) operation between queues.
The settings are global for all ports in the switch.
The displayed settings are:

Queue

The queue number (QoS class) for which the configuration below applies.

Enable

Controls whether RED is enabled for this queue.

Min. Threshold

Controls the lower RED threshold. If the average queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100.

Max. DP 1

Controls the drop probability for frames marked with Drop Precedence Level 1 when the average queue filling level is 100%. This value is restricted to 0-100.

Max. DP 2

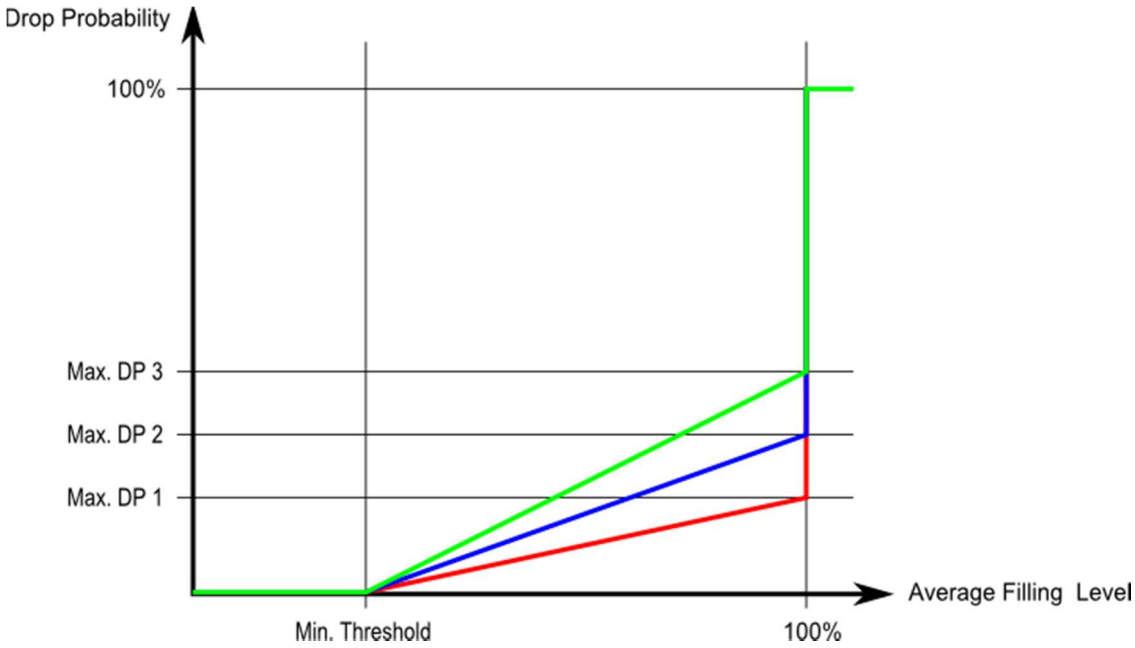
Controls the drop probability for frames marked with Drop Precedence Level 2 when the average queue filling level is 100%. This value is restricted to 0-100.

Max. DP 3

Controls the drop probability for frames marked with Drop Precedence Level 3 when the average queue filling level is 100%. This value is restricted to 0-100.

RED Drop Probability Function

The following illustration shows the drop probability function with associated parameters.



Max. DP 1-3 is the drop probability when the average queue filling level is 100%. Frames marked with Drop Precedence Level 0 are never dropped. Min. Threshold is the average queue filling level where the queues randomly start dropping frames. The drop probability for frames marked with Drop Precedence Level n increases linearly from zero (at Min. Threshold average queue filling level) to Max. DP n (at 100% average queue filling level).

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

Mirroring

Mirroring Configuration

To debug network problems, selected traffic can be copied, or mirrored, on a mirror port where a frame analyzer can be attached to analyze the frame flow.
The traffic to be copied on the mirror port is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).

Port to mirror to

Port to mirror also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.

Mirror Port Configuration

The following table is used for Rx and Tx enabling.

Port

The logical port for the settings contained in the same row.

Mode

Select mirror mode.
Rx only Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.
Tx only Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.
Disabled Neither frames transmitted nor frames received are mirrored.
Enabled Frames received and frames transmitted are mirrored on the mirror port.
Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror mirror port Tx frames. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

UPnP

UPnP Configuration

Configure UPnP on this page.

Mode

Indicates the UPnP operation mode. Possible modes are:
Enabled: Enable UPnP mode operation.
Disabled: Disable UPnP mode operation.
When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

TTL

The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 2.

Advertising Duration

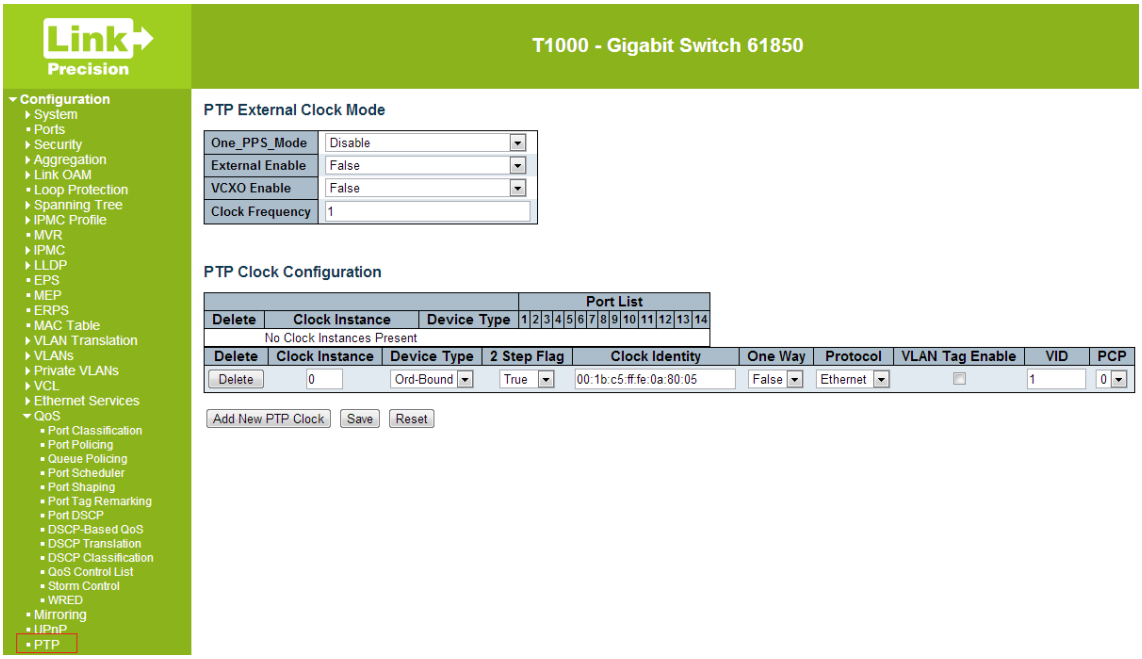
The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

Buttons

SAVE: Click to save changes.
RESET: Click to undo any changes made locally and revert to previously saved values.

PTP

PTP Clock Configuration



This page allows the user to configure and inspect the currentPTP clock settings.

One_pps_mode

This Selection box will allow you to select the One_pps_mode configuration.
The following values are possible:
1. Output : Enable the 1 pps clock output
2. Input : Enable the 1 pps clock input
3. Disable : Disable the 1 pps clock in/out-put

External Enable

This Selection box will allow you to configure the External Clock output.
The following values are possible:
1. True : Enable the external clock output
2. False : Disable the external clock output

VCXO_Enable

This Selection box will allow you to configure the External VCXO rate adjustment.
The following values are possible:
1. True : Enable the external VCXO rate adjustment
2. False : Disable the external VCXO rate adjustment

Clock Frequency

This will allow to set the Clock Frequency.
The possible range of values are 1 - 2000000 (1 - 2MHz)

PTP Clock Configuration

Delete
Check this box and click on 'Save' to delete the clock instance.

Clock Instance
Indicates the Instance of a particular Clock Instance [0..3].
Click on the Clock Instance number to edit the Clock details.

Device Type
Indicates the Type of the Clock Instance. There are five Device Types.
1. Ord-Bound - clock's Device Type is Ordinary-Boundary Clock.
2. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock.
3. E2e Transp - clock's Device Type is End to End Transparent Clock.
4. Master Only - clock's Device Type is Master Only.
. Slave Only - clock's Device Type is Slave Only.

Port List
Set check mark for each port configured for this Clock Instance.

2 Step Flag
Static member: defined by the system, true if two-step Sync events and Pdelay_Resp events are used

Clock Identity
It shows unique clock identifier

One Way
If true, one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

Protocol
Transport protocol used by the PTP protocol engine
ethernet PTP over Ethernet multicast
ip4multi PTP over IPv4 multicast
ip4uni PTP over IPv4 unicast
Note : IPv4 unicast protocol only works in Master only and Slave only clocks

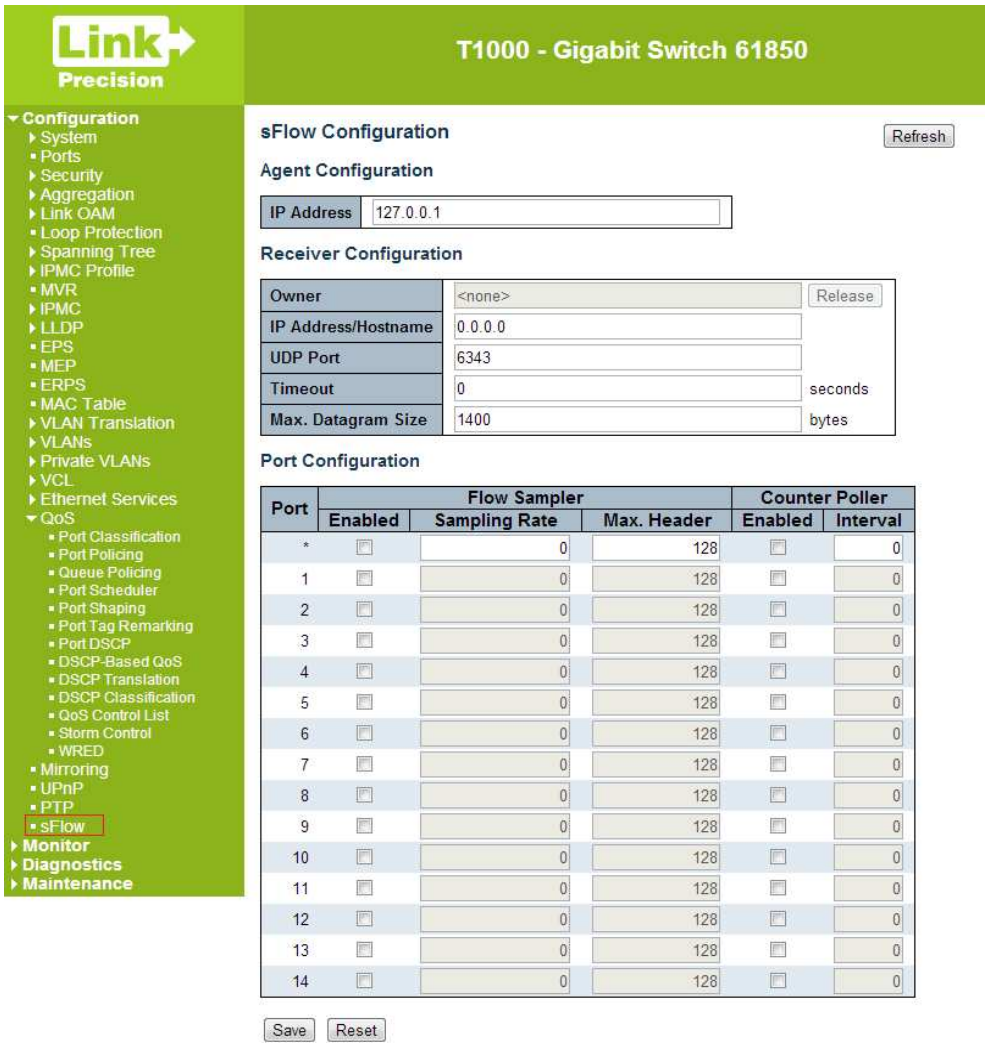
See parameter Device Type
In a unicast Slave only clock you also need configure which master clocks to request Announce and Sync messages from. See: Unicast Slave Configuration

VLAN Tag Enable
Enables the VLAN tagging for the PTP frames.
Note: Packets are only tagged if the port is configured for vlan tagging. i.e:
Port Type != Unaware and PortVLAN mode == None, and the port is member of the VLAN.

VID
VLAN Identifier used for tagging the PTP frames.

PCP
Priority Code Point value used for PTP frames.

sFlow



sFlow Configuration

This page allows for configuring sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers. sFlow configuration is not persisted to non-volatile memory, which means that a reboot will disable sFlow sampling.

Agent Configuration

IP Address
The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time.
Both IPv4 and IPv6 addresses are supported.

Receiver Configuration

Owner
Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:
· If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
· If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
· If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.
If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.
The button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

IP Address/Hostname
The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

UDP Port
The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.

Timeout
The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.

Max. Datagram Size
The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Port Configuration

Port
The port number for which the configuration below applies.

Flow Sampler Enabled
Enables/disables flow sampling on this port.

Flow Sampler Sampling Rate
The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port.
Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.

Flow Sampler Max. Header
The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes.

If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

Counter Poller Enabled

Enables/disables counter polling on this port.

Counter Poller Interval

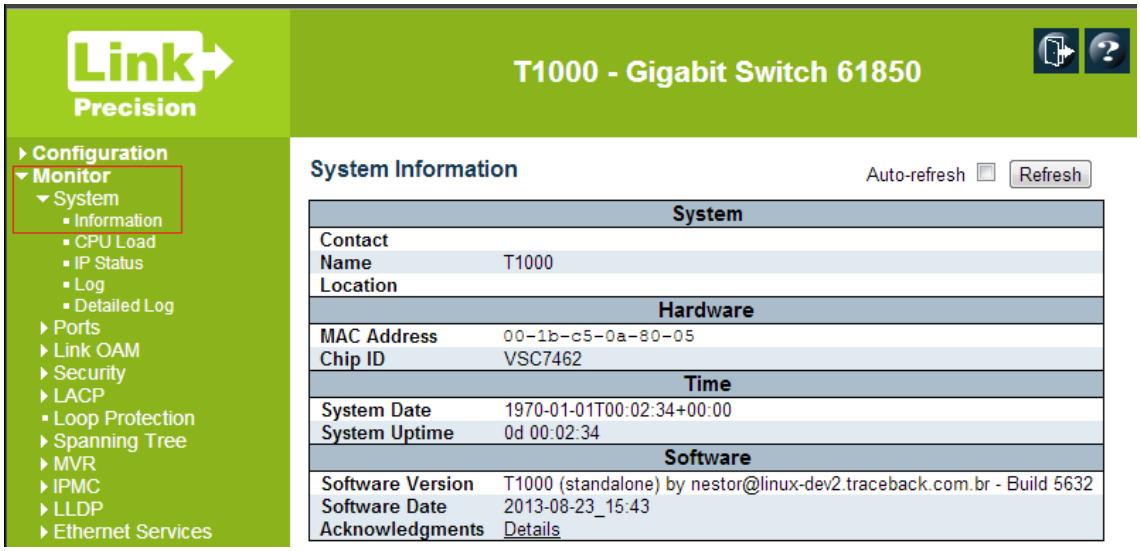
With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

Buttons

RELEASE: See description under Owner.
REFRESH: Click to refresh the page. Note that unsaved changes will be lost.
SAVE: Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory.
RESET: Click to undo any changes made locally and revert to previously saved values.

System

System Information



The switch system information is provided here.

Contact

The system contact configured in Configuration | System | Information | System Contact.

Name

The system name configured in Configuration | System | Information | System Name.

Location

The system location configured in Configuration | System | Information | System Location.

MAC Address

The MAC Address of this switch.

Chip ID

The Chip ID of this switch.

System Date

The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.

System Uptime

The period of time the device has been operational.

Software Version

The software version of this switch.

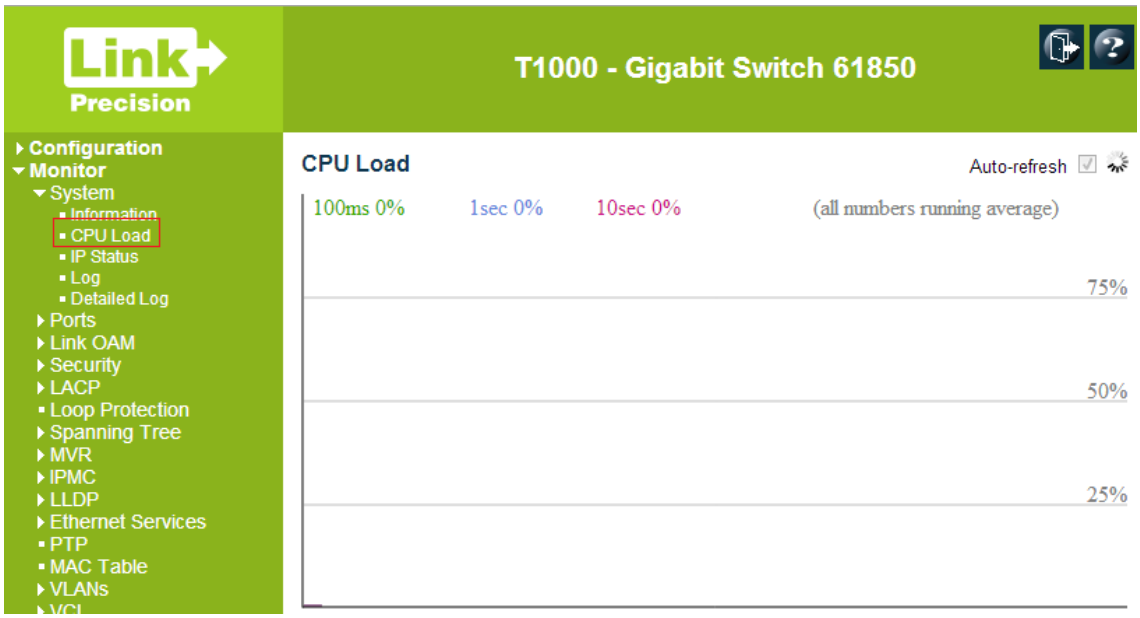
Software Date

The date when the switch software was produced.

Buttons

AUTO REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page.

CPU Load

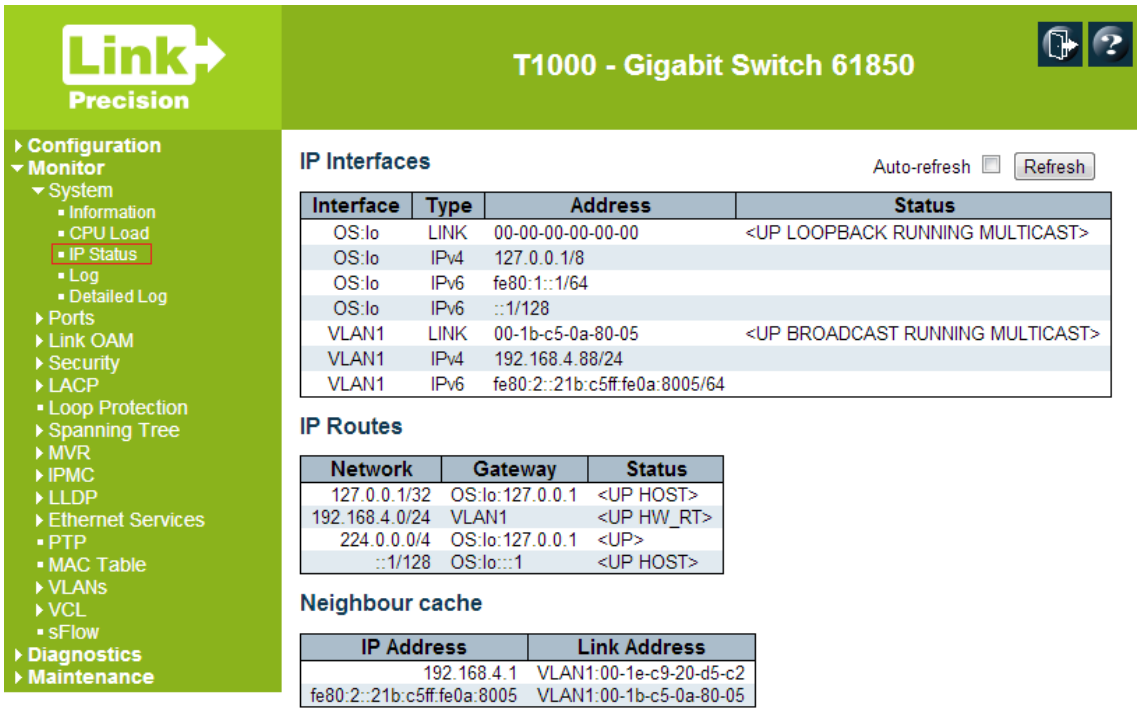


This page displays the CPU load, using an SVG graph.
The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.
In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

Buttons

Auto-Refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

IP Status



This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbour cache (ARP cache) status.

IP Interfaces

Interface
The name of the interface.

Type
The address type of the entry. This may be LINK orIPv4.

Address
The current address of the interface (of the given type).

Status
The status flags of the interface (and/or address).

IP Routes

Network
The destination IP network or host address of this route.

Gateway
The gateway address of this route.

Status
The status flags of the route.

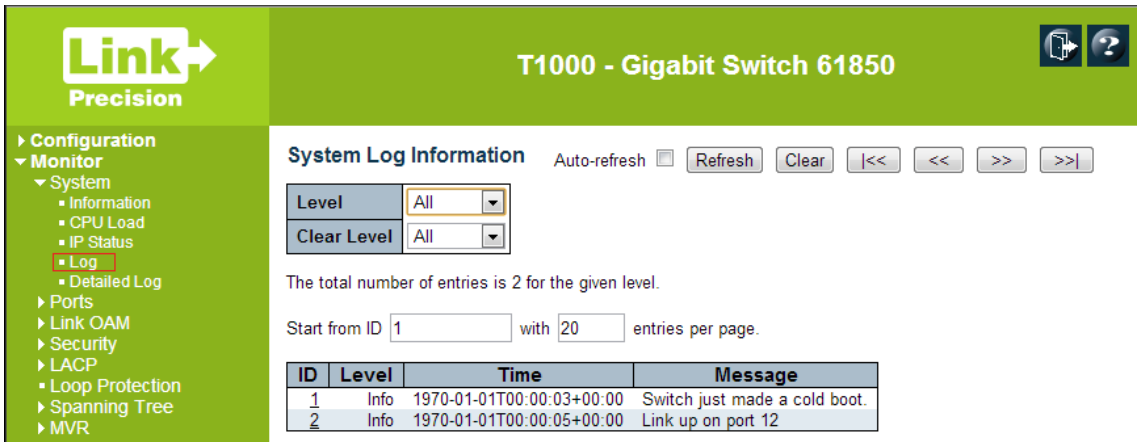
Neighbour cache

IP Address
The IP address of the entry.

Link Address
The Link (MAC) address for which a binding to the IP address given exist..

Buttons
: Click to refresh the page immediately.
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

System Log Information



The switch system log information is provided here.

ID

The ID (>= 1) of the system log entry.

Level

The level of the system log entry. The following level types are supported:
Info: Information level of the system log.
Warning: Warning level of the system log.
Error: Error level of the system log.
All: All levels.

Time

The time of the system log entry.

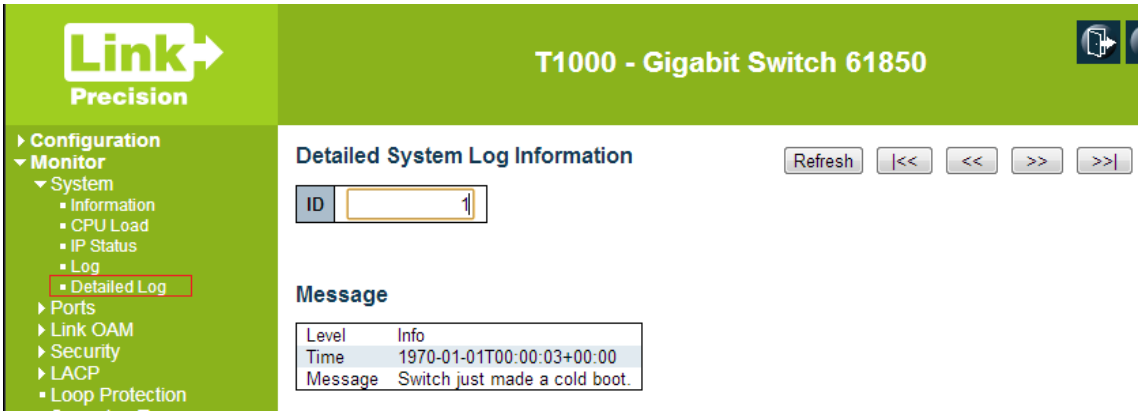
Message

The message of the system log entry.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Updates the system log entries, starting from the current entry ID.
CLEAR: Flushes the selected log entries.
|<<: Updates the system log entries, starting from the first available entry ID.
<<: Updates the system log entries, ending at the last entry currently displayed.
>>: Updates the system log entries, starting from the last entry currently displayed.
>>|: Updates the system log entries, ending at the last available entry ID.

Detailed System Log Information



The switch system detailed log information is provided here.

ID

The ID (>= 1) of the system log entry.

Message

The detailed message of the system log entry.

Buttons

REFRESH: Updates the system log entry to the current entry ID.
|<<: Updates the system log entry to the first available entry ID.
:<< Updates the system log entry to the previous available entry ID.
>>: Updates the system log entry to the next available entry ID.
>>|: Updates the system log entry to the last available entry ID.

Ports

Port State

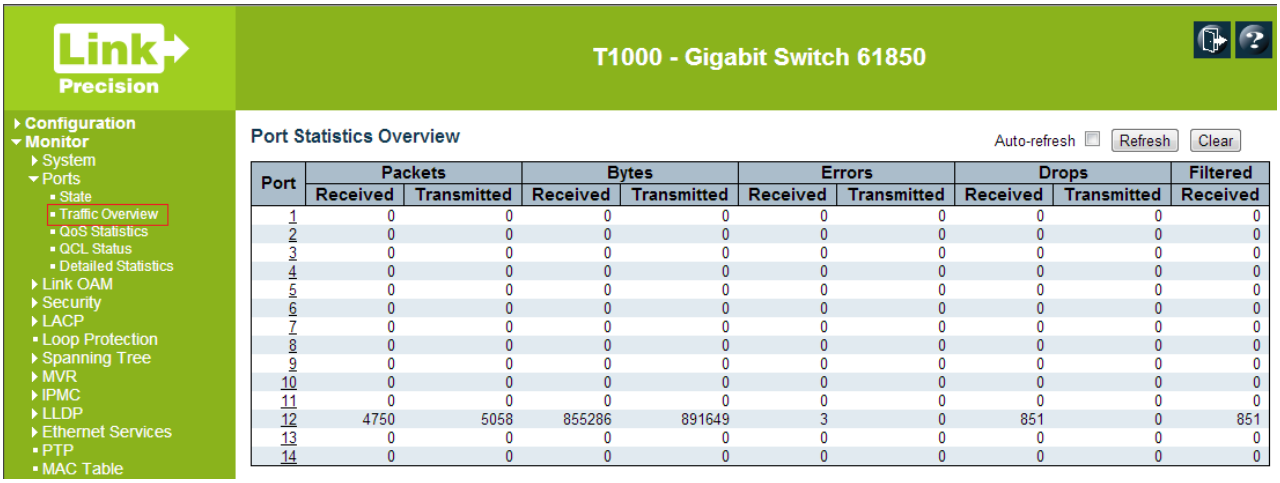
This page provides an overview of the current switch port states.
The port states are illustrated as follows:

STATE / PORTS	Disabled	Down	Link
RJ4 ports			
SFP ports			
X2 ports			

Buttons

AUTO-REFRESH : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page.

Port Statistics Traffic Overview


Link Precision
T1000 - Gigabit Switch 61850
Configuration
Monitor
System
Ports
State
Traffic Overview
QoS Statistics
QCL Status
Detailed Statistics
Link OAM
Security
LACP
Loop Protection
Spanning Tree
MVR
IPMC
LLDP
Ethernet Services
PTP
MAC Table
Port Statistics Overview
Auto-refresh
Refresh
Clear
Port
Packets
Bytes
Errors
Drops
Filtered
Received
Transmitted
1 0 0 0 0 0 0 0 0 0
2 0 0 0 0 0 0 0 0 0
3 0 0 0 0 0 0 0 0 0
4 0 0 0 0 0 0 0 0 0
5 0 0 0 0 0 0 0 0 0
6 0 0 0 0 0 0 0 0 0
7 0 0 0 0 0 0 0 0 0
8 0 0 0 0 0 0 0 0 0
9 0 0 0 0 0 0 0 0 0
10 0 0 0 0 0 0 0 0 0
11 0 0 0 0 0 0 0 0 0
12 4750 5058 855286 891649 3 0 851 0 851
13 0 0 0 0 0 0 0 0 0
14 0 0 0 0 0 0 0 0 0

This page provides an overview of general traffic statistics for all switch ports.
The displayed counters are:

Port

The logical port for the settings contained in the same row.

Packets

The number of received and transmitted packets per port.

Bytes

The number of received and transmitted bytes per port.

Errors

The number of frames received in error and the number of incomplete transmissions per port.

Drops

The number of frames discarded due to ingress or egress congestion.

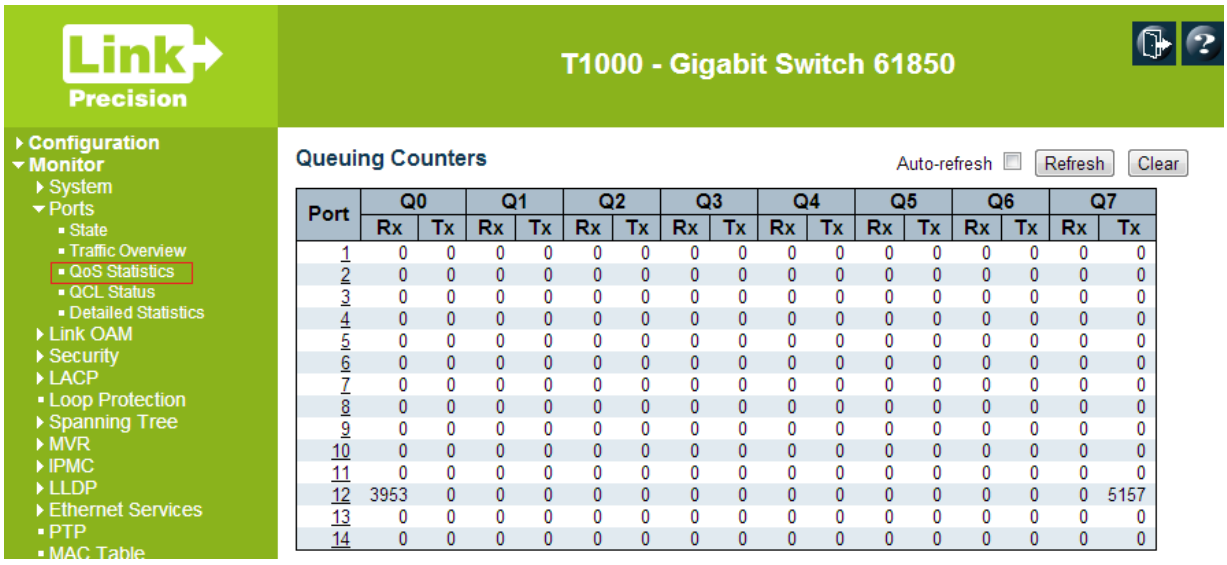
Filtered

The number of received frames filtered by the forwarding process.

Buttons

REFRESH: Click to refresh the page immediately.
CLEAR: Clears the counters for all ports.
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

QoS Statistics



Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	3953	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5157
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

This page provides statistics for the different queues for all switch ports.
The displayed counters are:

Port

The logical port for the settings contained in the same row.

Qn

There are 8 QoS queues per port. Q0 is the lowest priority queue.

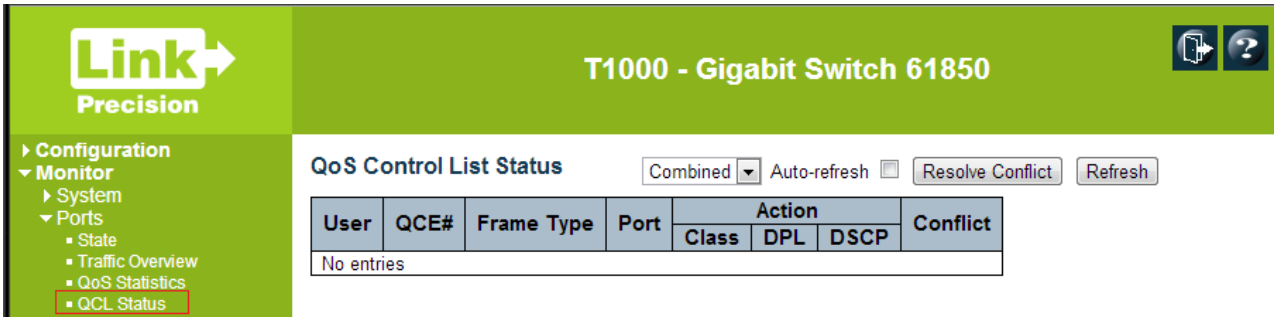
Rx/Tx

The number of received and transmitted packets per queue.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
CLEAR: Clears the counters for all ports.

QCL Status



This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 26 on each switch.

User

Indicates the QCL user.

QCE#

Indicates the index of QCE.

Frame Type

Indicates the type of frame to look for incoming frames. Possible frame types are:
Any: The QCE will match all frame type.
Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.
LLC: Only (LLC) frames are allowed.
SNAP: Only (SNAP) frames are allowed.
IPv4: The QCE will match only IPV4 frames.
IPv6: The QCE will match only IPV6 frames.

Port

Indicates the list of ports configured with the QCE.

Action

Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.
There are three action fields: Class, DPL and DSCP.
Class: Classified QoS class; if a frame matches the QCE it will be put in the queue.
DPL: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column.
DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.

Conflict

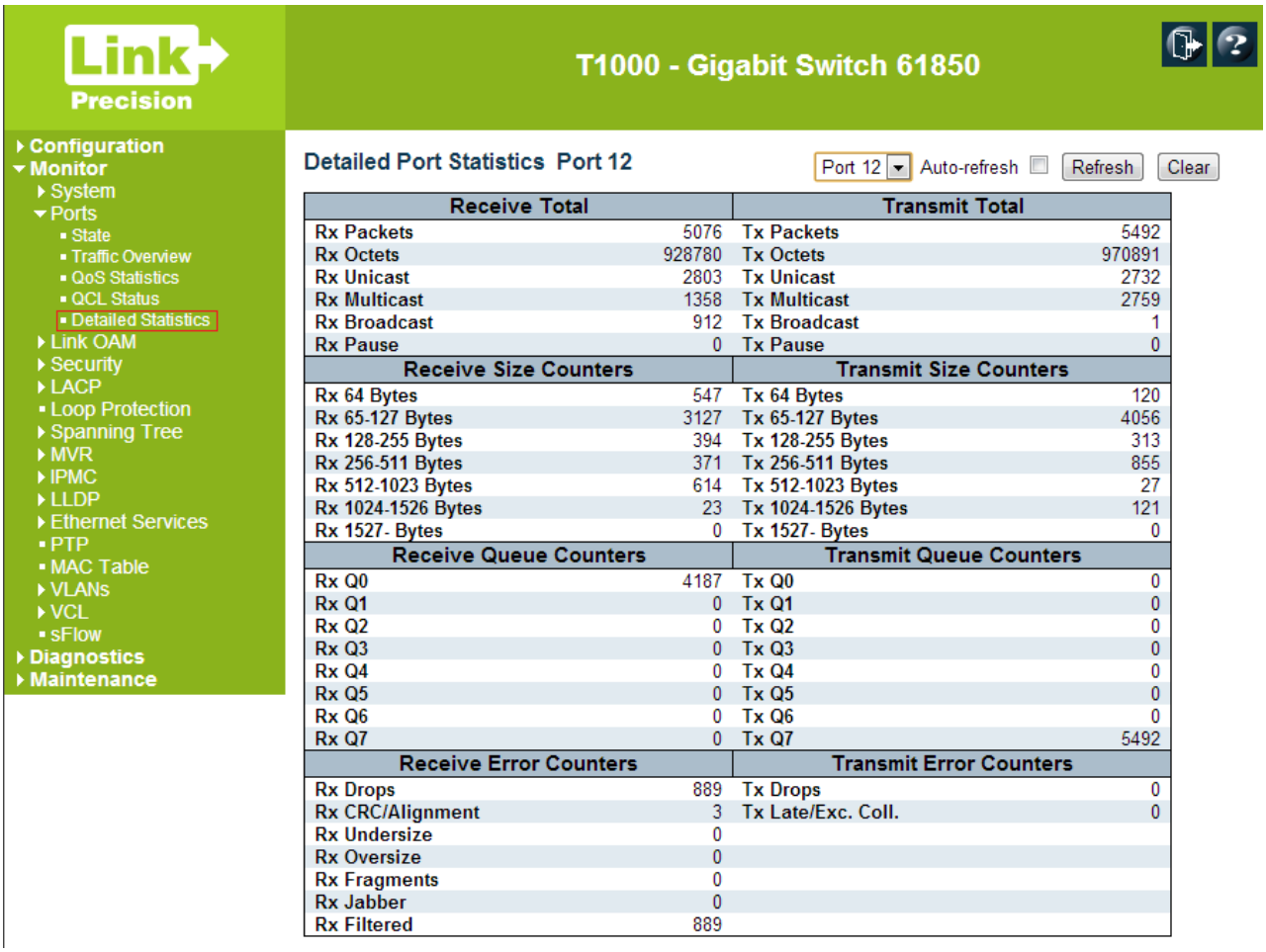
Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

Buttons

: Select the QCL status from this drop down list.

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
RESOLVE CONFLICT: Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.
REFRESH: Click to refresh the page.

Detailed Port Statistics



Receive Total		Transmit Total	
Rx Packets	5076	Tx Packets	5492
Rx Octets	928780	Tx Octets	970891
Rx Unicast	2803	Tx Unicast	2732
Rx Multicast	1358	Tx Multicast	2759
Rx Broadcast	912	Tx Broadcast	1
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	547	Tx 64 Bytes	120
Rx 65-127 Bytes	3127	Tx 65-127 Bytes	4056
Rx 128-255 Bytes	394	Tx 128-255 Bytes	313
Rx 256-511 Bytes	371	Tx 256-511 Bytes	855
Rx 512-1023 Bytes	614	Tx 512-1023 Bytes	27
Rx 1024-1526 Bytes	23	Tx 1024-1526 Bytes	121
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	4187	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	5492
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	889	Tx Drops	0
Rx CRC/Alignment	3	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	889		

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.
The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Receive Total and Transmit Total

Rx and Tx Packets

The number of received and transmitted (good and bad) packets.

Rx and Tx Octets

The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Rx and Tx Unicast

The number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast

The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast
The number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause
A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters
The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters
The number of received and transmitted packets per input and output queue.

Receive Error Counters

Rx Drops
The number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment
The number of frames received with CRC or alignment errors.

Rx Undersize
The number of short 1 frames received with valid CRC.

Rx Oversize
The number of long 2 frames received with valid CRC.

Rx Fragments
The number of short 1 frames received with invalid CRC.

Rx Jabber
The number of long 2 frames received with invalid CRC.

Rx Filtered
The number of received frames filtered by the forwarding process.
1 Short frames are frames that are smaller than 64 bytes.
2 Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

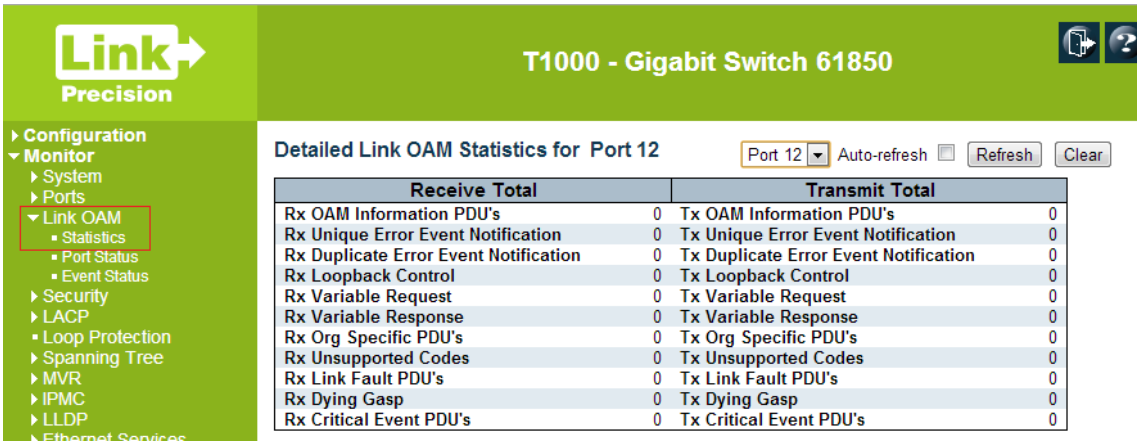
Tx Drops
The number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.
The number of frames dropped due to excessive or late collisions.

Buttons
The port select box determines which port is affected by clicking the buttons.
REFRESH: Click to refresh the page immediately.
CLEAR: Clears the counters for the selected port.
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Link OAM

Detailed Link OAM Port Statistics



This page provides detailed OAM traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.
The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counter can occur at re-initialization of the management system.

Receive Total and Transmit Total

Rx and Tx OAM Information PDU's

The number of received and transmitted OAM Information PDU's. Discontinuities of this counter can occur at re-initialization of the management system.

Rx and Tx Unique Error Event Notification

A count of the number of unique Event OAMPDUs received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Duplicate Error Event Notification

A count of the number of duplicate Event OAMPDUs received and transmitted on this interface. Event Notification OAMPDUs may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Loopback Control

A count of the number of Loopback Control OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Request
A count of the number of Variable Request OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Response
A count of the number of Variable Response OAMPDUs received and transmitted on this interface.

Rx and Tx Org Specific PDU's
A count of the number of Organization Specific OAMPDUs transmitted on this interface.

Rx and Tx Unsupported Codes
A count of the number of OAMPDUs transmitted on this interface with an unsupported op-code.

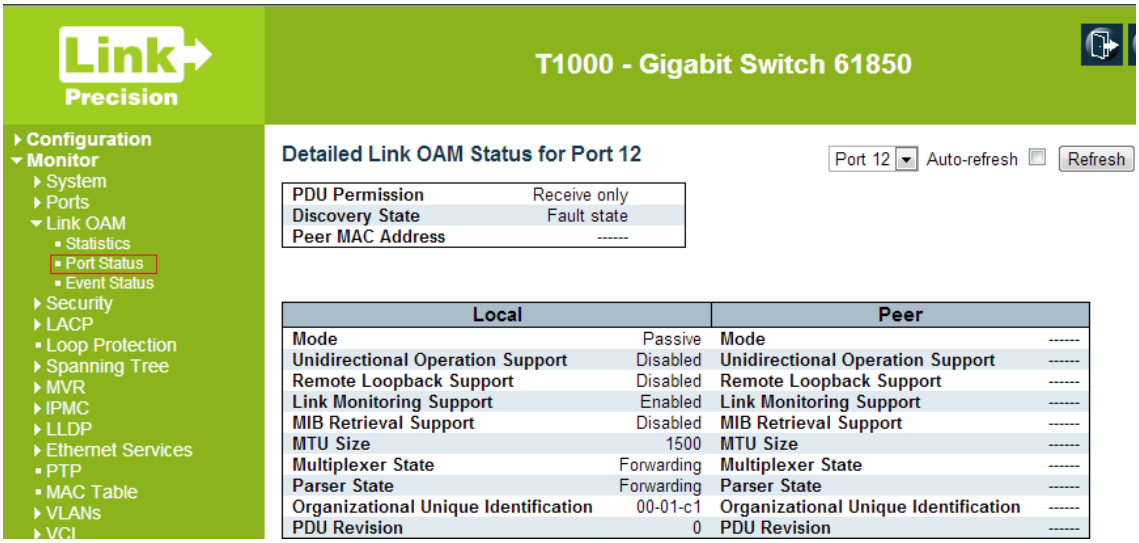
Rx and Tx Link fault PDU's
A count of the number of Link fault PDU's received and transmitted on this interface.

Rx and Tx Dying Gasp
A count of the number of Dying Gasp events received and transmitted on this interface.

Rx and Tx Critical Event PDU's
A count of the number of Critical event PDU's received and transmitted on this interface.

Buttons
The port select box determines which port is affected by clicking the buttons.
AUTO-REFRESH: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
CLEAR: Clears the counters for the selected port.

Link OAM Port Configuration Status



This page provides Link OAM configuration operational status.
The displayed fields shows the active configuration status for the selected port.

Local and Peer

Mode
The Mode in which the Link OAM is operating, Active or Passive.

Unidirectional Operation Support
This feature is not available to be configured by the user. The status of this configuration is retrieved from the PHY.

Remote Loopback Support
If status is enabled, DTE is capable of OAM remote loopback mode.

Link Monitoring Support
If status is enabled, DTE supports interpreting Link Events.

MIB Retrieval Support
If status ie enabled DTE supports sending Variable Response OAMPDUs.

MTU Size
It represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remotes Maximum PDU Size and the smaller of the two is used.

Multiplexer State
When in forwarding state, the Device is forwarding non-OAMPDUs to the lower sublayer. Incase of discarding, the device discards all the non-OAMPDU's.

Parser State
When in forwarding state, Device is forwarding non-OAMPDUs to higher sublayer. When in loopback, Device is looping back non-OAMPDUs to the lower sublayer. When in discarding state, Device is discarding non-OAMPDUs.

Organizational Unique Identification
24-bit Organizationally Unique Identifier of the vendor.

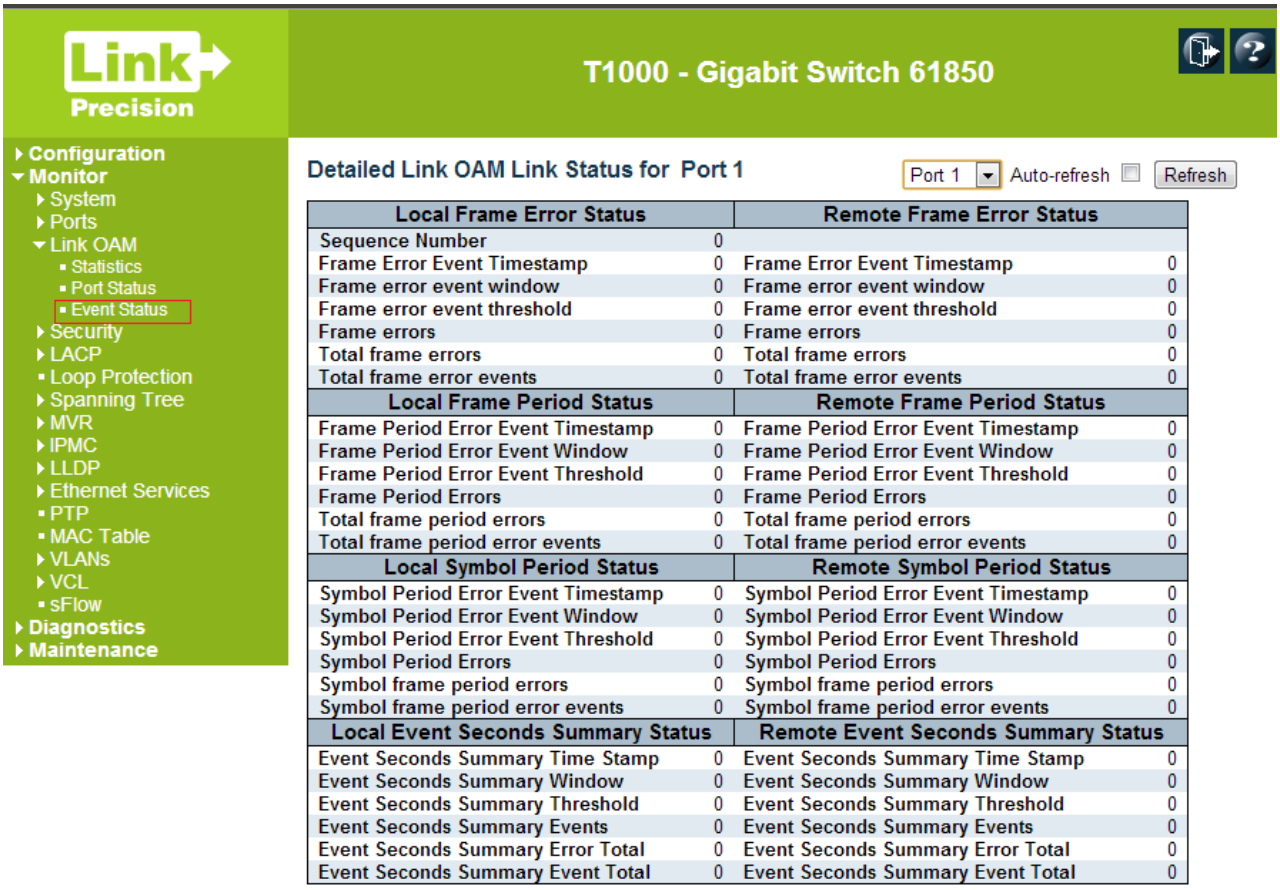
PDU Revision
It indicates the current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV doesn't need to be parsed as nothing in it has changed).

PDU Permission
This field is available only for the Local DTE. It displays the current permission rules set for the local DTE. Possible values are "Link fault","Receive only", "Information exchange only","ANY".

Discovery State
Displays the current state of the discovery process. Possible states are Fault state, Active state, Passive state, SEND_LOCAL_REMOTE_STATE, SEND_LOCAL_REMOTE_OK_STATE, SEND_ANY_STATE.

Buttons
The port select box determines which port is affected by clicking the buttons.
REFRESH: Click to refresh the page immediately.
AUTO-REFRESH: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Link OAM Link Event Status



Local Frame Error Status		Remote Frame Error Status	
Sequence Number	0		
Frame Error Event Timestamp	0	Frame Error Event Timestamp	0
Frame error event window	0	Frame error event window	0
Frame error event threshold	0	Frame error event threshold	0
Frame errors	0	Frame errors	0
Total frame errors	0	Total frame errors	0
Total frame error events	0	Total frame error events	0
Local Frame Period Status		**Remote Frame Period Status**	
Frame Period Error Event Timestamp	0	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	0	Frame Period Error Event Window	0
Frame Period Error Event Threshold	0	Frame Period Error Event Threshold	0
Frame Period Errors	0	Frame Period Errors	0
Total frame period errors	0	Total frame period errors	0
Total frame period error events	0	Total frame period error events	0
Local Symbol Period Status		**Remote Symbol Period Status**	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0
Symbol Period Error Event Threshold	0	Symbol Period Error Event Threshold	0
Symbol Period Errors	0	Symbol Period Errors	0
Symbol frame period errors	0	Symbol frame period errors	0
Symbol frame period error events	0	Symbol frame period error events	0
Local Event Seconds Summary Status		**Remote Event Seconds Summary Status**	
Event Seconds Summary Time Stamp	0	Event Seconds Summary Time Stamp	0
Event Seconds Summary Window	0	Event Seconds Summary Window	0
Event Seconds Summary Threshold	0	Event Seconds Summary Threshold	0
Event Seconds Summary Events	0	Event Seconds Summary Events	0
Event Seconds Summary Error Total	0	Event Seconds Summary Error Total	0
Event Seconds Summary Event Total	0	Event Seconds Summary Event Total	0

This page allows the user to inspect the current Link OAM Link Event configurations, and change them as well.
The left pane displays the Event status for the Local OAM unit while the right pane displays the status for the Peer for the respective port.

Port

The switch port number.

Sequence Number

This two-octet field indicates the total number of events occurred at the remote end.

Frame Error Event Timestamp

This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame error event window

This two-octet field indicates the duration of the period in terms of 100 ms intervals. 1) The default value is one second. 2) The lower bound is one second. 3) The upper bound is one minute.

Frame error event threshold

This four-octet field indicates the number of detected errored frames in the period is required to be equal to or greater than in order for the event to be generated. 1) The default value is one frame error. 2) The lower bound is zero frame errors. 3) The upper bound is unspecified.

Frame errors
This four-octet field indicates the number of detected errored frames in the period.

Total frame errors
This eight-octet field indicates the sum of errored frames that have been detected since the OAM sublayer was reset.

Total frame error events
This four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sublayer was reset.

Frame Period Error Event Timestamp
This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame Period Error Event Window
This four-octet field indicates the duration of period in terms of frames.

Frame Period Error Event Threshold
This four-octet field indicates the number of errored frames in the period is required to be equal to or greater than in order for the event to be generated.

Frame Period Errors
This four-octet field indicates the number of frame errors in the period.

Total frame period errors
This eight-octet field indicates the sum of frame errors that have been detected since the OAM sublayer was reset.

Total frame period error events
This four-octet field indicates the number of Errored Frame Period Event TLVs that have been generated since the OAM sublayer was reset.

Symbol Period Error Event Timestamp
This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Symbol Period Error Event Window
This eight-octet field indicates the number of symbols in the period.

Symbol Period Error Event Threshold
This eight-octet field indicates the number of errored symbols in the period is required to be equal to or greater than in order for the event to be generated.

Symbol Period Errors
This eight-octet field indicates the number of symbol errors in the period.

Symbol frame period errors
This eight-octet field indicates the sum of symbol errors since the OAM sublayer was reset.

Symbol frame period error events

This four-octet field indicates the number of Errored Symbol Period Event TLVs that have been generated since the OAM sublayer was reset.

Event Seconds Summary Time Stamp

This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Event Seconds Summary Window

This two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Event Seconds Summary Threshold

This two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 16-bit unsigned integer.

Event Seconds Summary Events

This two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.

Event Seconds Summary Error Total

This four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sublayer was reset.

Event Seconds Summary Event Total

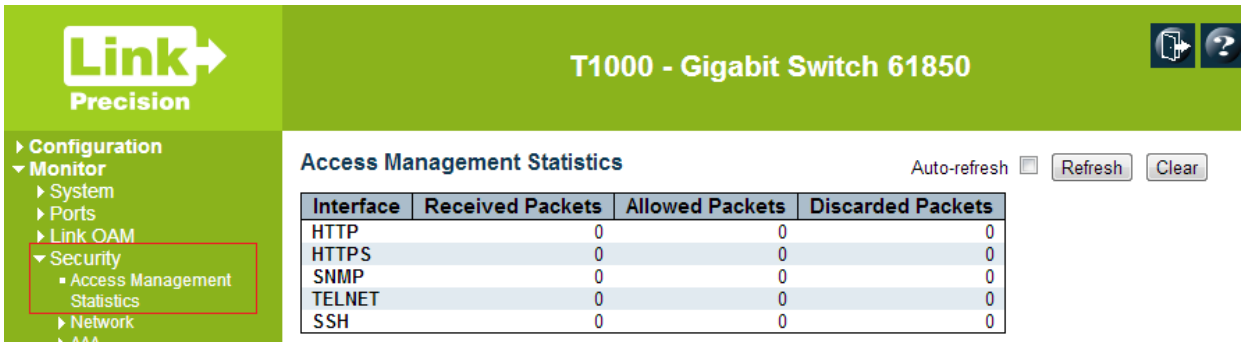
This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sublayer was reset, encoded as a 32bit unsigned integer.

Buttons

The port select box determines which port is affected by clicking the buttons.
AUTO-REFRESH: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page.
CLEAR: Click to clear the data.

Security

Access Management Statistics



This page provides statistics for access management.

Interface

The interface type through which the remote host can access the switch.

Received Packets

Number of received packets from the interface when access management mode is enabled.

Allowed Packets

Number of allowed packets from the interface when access management mode is enabled.

Discarded Packets

Number of discarded packets from the interface when access management mode is enabled.

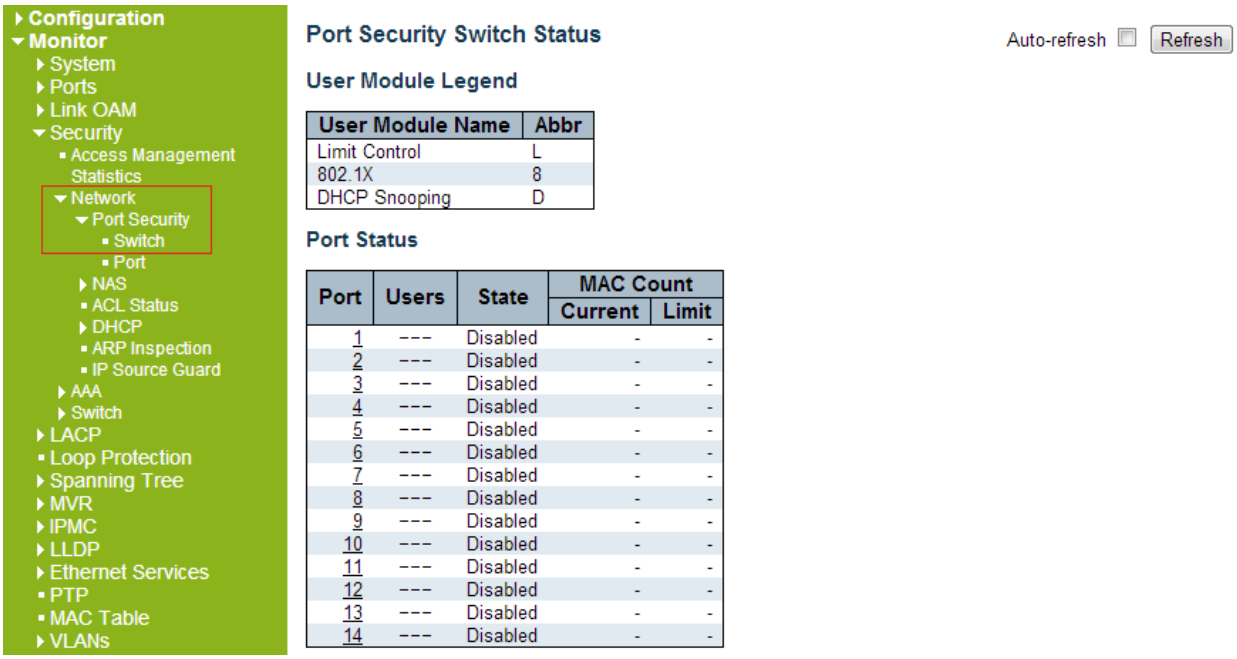
Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
CLEAR: Clear all statistics.

Network

Port Security

Port Security Switch Status



This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

User Module Legend

The legend shows all user modules that may request Port Security services.

User Module Name

The full name of a module that may request Port Security services.

Abbr

A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

Port Status

The table has one row for each port on the switch and a number of columns, which are:

Port
The port number for which the status applies. Click the port number to see the status for this particular port.

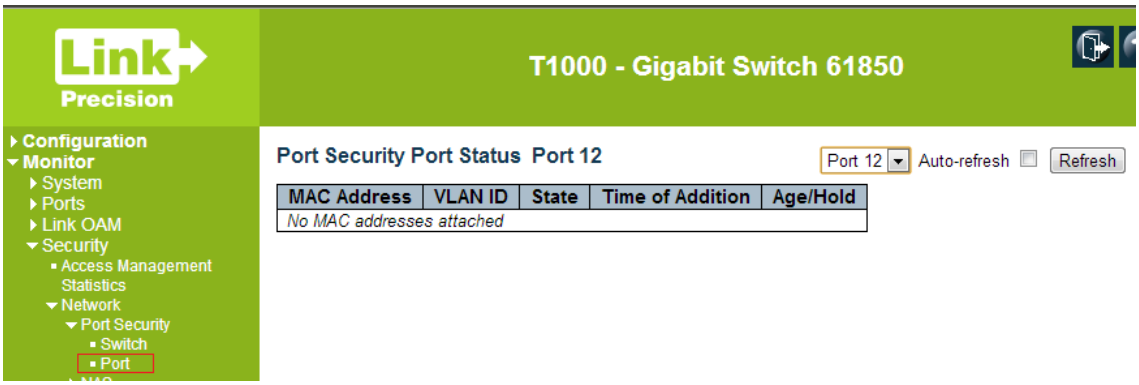
Users
Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.

State
Shows the current state of the port. It can take one of four values:
Disabled: No user modules are currently using the Port Security service.
Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.
Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.
Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

MAC Count (Current, Limit)
The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.
If no user modules are enabled on the port, the Current column will show a dash (-).
If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Buttons
AUTO-REFRESH : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.

Port Security Port Status



This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

MAC Address & VLAN ID

The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

State

Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition

Shows the date and time when this MAC address was first seen on the port.

Age/Hold

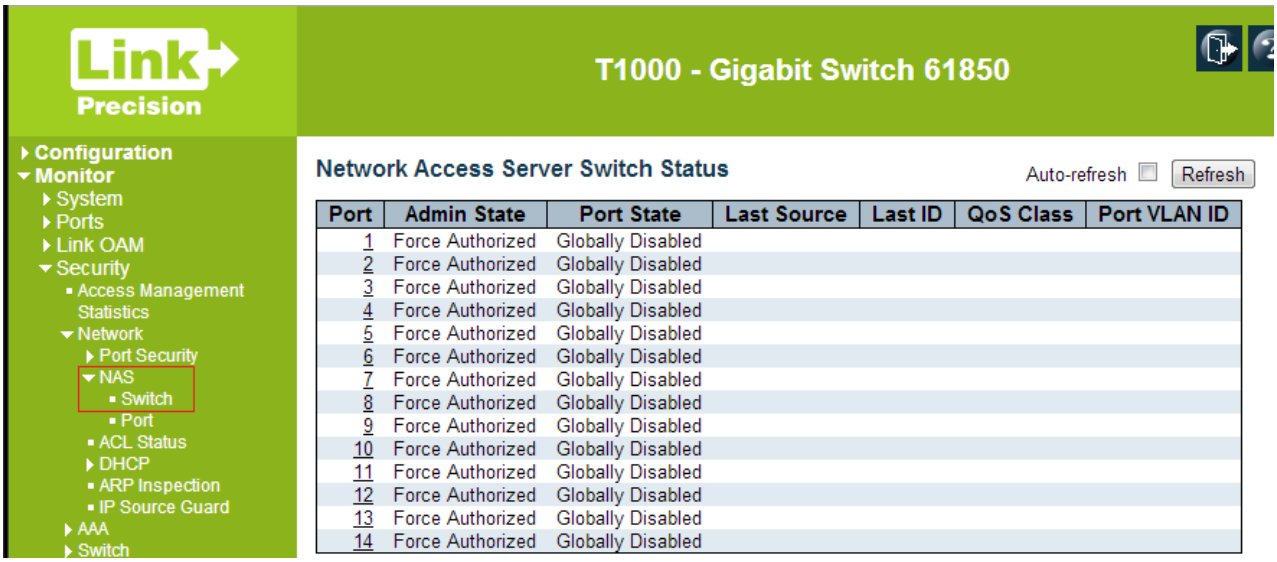
If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.
If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

Use the port select box to select which port to show status for.
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.

NAS

NAS Switch Status



This page provides an overview of the current NAS port states.

Port

The switch port number. Click to navigate to detailed NAS statistics for this port.

Admin State

The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State

The current state of the port. Refer to NAS Port State for a description of the individual states.

Last Source

The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID

The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

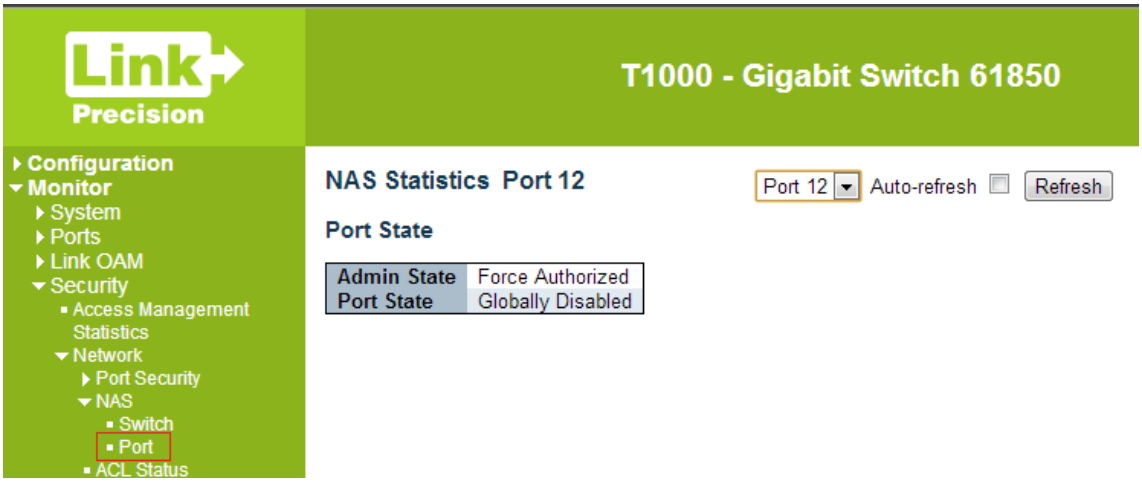
QoS Class

QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID

The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.
If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.
If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANshere.

NAS Statistics Port



This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only .
Use the port select box to select which port details to be displayed.

Port State

Admin State
The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State
The current state of the port. Refer to NAS Port State for a description of the individual states.

QoS Class
The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

Port VLAN ID
The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.
If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.
If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANshere.

Port Counters

EAPOL Counters
These supplicant frame counters are available for the following administrative states:
· Force Authorized
· Force Unauthorized
· Port-based 802.1X
· Single 802.1X
· Multi 802.1X

DIRECTION	NAME	IEEE NAME	DESCRIPTION
Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	Invalid Length	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted

		by the switch.

Backend Server Counters

These backend (RADIUS) frame counters are available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

DIRECTION	NAME	IEEE NAME	DESCRIPTION
Rx	Access Challenges	dot1xAuthBackendAccessChallenges	802.1X-based: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
Rx	Other Requests	dot1xAuthBackendOtherRequestsToSupplicant	802.1X-based: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. MAC-based: Not applicable.
Rx	Auth. Successes	dot1xAuthBackendAuthSuccesses	802.1X- and MAC-based: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/clienthas successfully authenticated to the backend server.
Rx	Auth. Failures	dot1xAuthBackendAuthFails	802.1X- and MAC-based: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/clienthas not authenticated to the backend server.
Tx	Responses	dot1xAuthBackendResponses	802.1X-based: Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch

	attempted communication with the backend server. Possible retransmissions are not counted. MAC-based: Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

Last Supplicant/Client Info

Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

DIRECTION	NAME	IEEE NAME	DESCRIPTION
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.	MAC Address
VLAN ID	-	The VLAN ID on which the last frame from the last supplicant/clientwas received.	VLAN ID
Version	dot1xAuthLastEapolFrameVersion	802.1X-based: The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable.	Version
Identity	-	802.1X-based: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. MAC-based: Not applicable.	Identity

Selected Counters

The Selected Counters table is visible when the port is in one of the following administrative states:

- Multi 802.1X
- MAC-based Auth.

The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of theattached MAC Addresses from the table below.

Attached MAC Addresses

Identity
Shows the identity of the supplicant, as received in the Response Identity EAPOL frame.
Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached.
This column is not available for MAC-based Auth.

MAC Address
For Multi 802.1X, this column holds the MAC address of the attached supplicant.
For MAC-based Auth., this column holds the MAC address of the attached client.
Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.

VLAN ID
This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

State
The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.

Last Authentication
Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

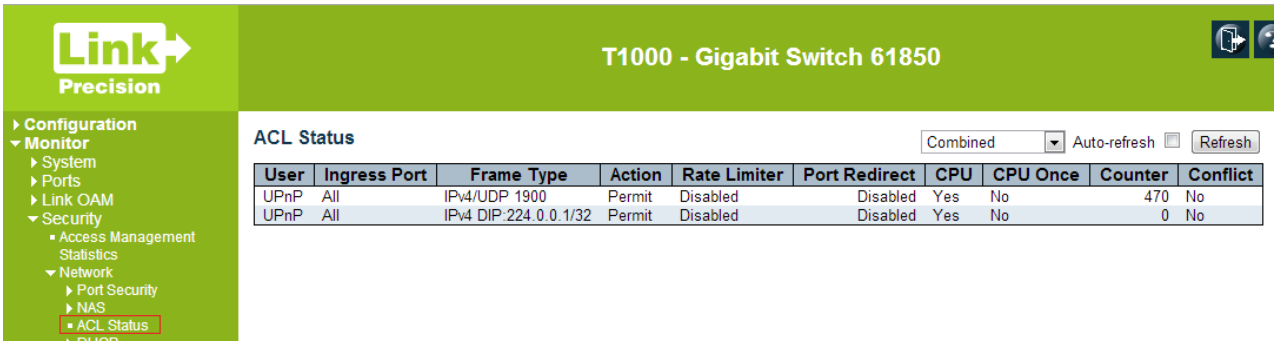
Buttons
The port select box determines which port is affected when clicking the buttons.
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Click to refresh the page immediately.
This button is available in the following modes:
· Force Authorized
· Force Unauthorized
· Port-based 802.1X
· Single 802.1X

Click to clear the counters for the selected port.
This button is available in the following modes:
· Multi 802.1X
· MAC-based Auth.X

Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however.
This button is available in the following modes:
· Multi 802.1X
· MAC-based Auth.X

Click to clear only the currently selected client's counters.

ACL Status


Link Precision
T1000 - Gigabit Switch 61850
Configuration
Monitor
System
Ports
Link OAM
Security
Access Management
Statistics
Network
Port Security
NAS
ACL Status
ACL Status
Combined
Auto-refresh
Refresh
User | Ingress Port | Frame Type | Action | Rate Limiter | Port Redirect | CPU | CPU Once | Counter | Conflict
UPnP | All | IPv4/UDP 1900 | Permit | Disabled | Disabled | Yes | No | 470 | No
UPnP | All | IPv4 DIP:224.0.0.1/32 | Permit | Disabled | Disabled | Yes | No | 0 | No

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 12 on each switch.

User

Indicates the ACL user.

Ingress Port

Indicates the ingress port of the ACE. Possible values are:
All: The ACE will match all ingress port.
Port: The ACE will match a specific ingress port.

Frame Type

Indicates the frame type of the ACE. Possible values are:
Any: The ACE will match any frame type.
EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IPand ARP frames.
ARP: The ACE will match ARP/RARP frames.
IPv4: The ACE will match all IPv4 frames.
IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.
IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.
IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.
IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
IPv6: The ACE will match all IPv6 standard frames.

Action

Indicates the forwarding action of the ACE.
Permit: Frames matching the ACE may be forwarded and learned.
Deny: Frames matching the ACE are dropped.

Rate Limiter

Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

CPU

Forward packet that matched the specific ACE to CPU.

CPU Once

Forward first packet that matched the specific ACE to CPU.

Counter

The counter indicates the number of times the ACE was hit by a frame.

Conflict

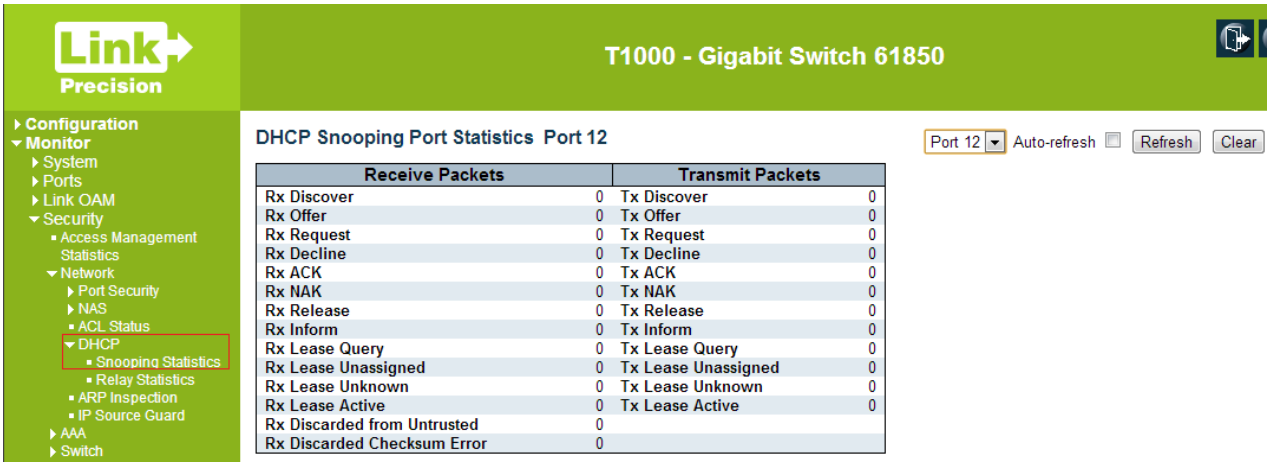
Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons

The select box determines which ACL user is affected by clicking the buttons.
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page.

DHCP

DHCP Snooping Statistics



This page provides statistics for DHCP snooping. The statistics doesn't count the DHCP packets for system DHCP client or DHCP relay mode is enabled.

Receive and Transmit Packets

Rx and Tx Discover
The number of discover (option 3 with value 1) packets received and transmitted.

Rx and Tx Offer
The number of offer (option 3 with value 2) packets received and transmitted.

Rx and Tx Request
The number of request (option 3 with value 3) packets received and transmitted.

Rx and Tx Decline
The number of decline (option 3 with value 4) packets received and transmitted.

Rx and Tx ACK
The number of ACK (option 3 with value) packets received and transmitted.

Rx and Tx NAK
The number of NAK (option 3 with value 6) packets received and transmitted.

Rx and Tx Release
The number of release (option 3 with value 7) packets received and transmitted.

Rx and Tx Inform
The number of inform (option 3 with value 8) packets received and transmitted.

Rx and Tx Lease Query
The number of lease query (option 3 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned
The number of lease unassigned (option 3 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown
The number of lease unknown (option 3 with value 12) packets received and transmitted.

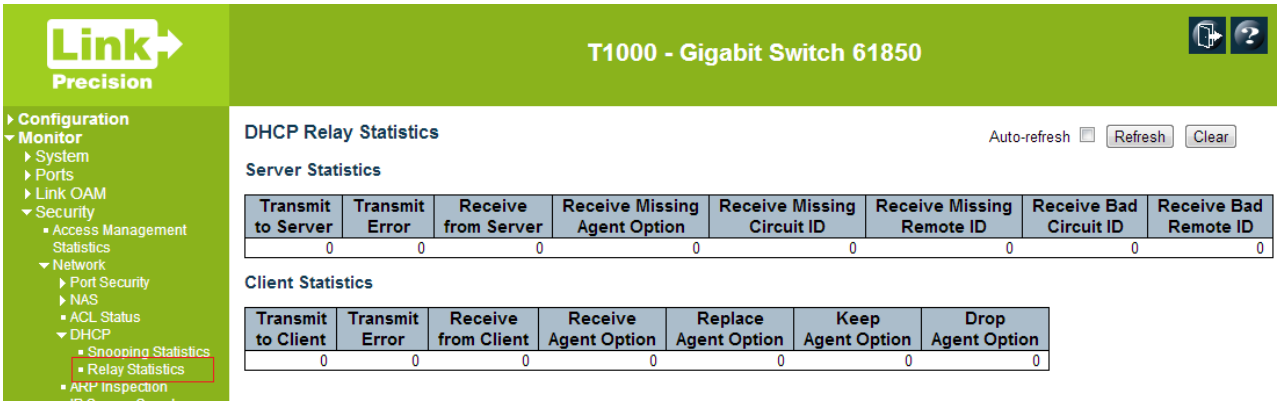
Rx and Tx Lease Active
The number of lease active (option 3 with value 13) packets received and transmitted.

Rx Discarded from Untrusted
The number of discarded packet that are coming from untrusted port.

Rx Discarded checksum error
The number of discard packet that IP/UDP checksum is error.

Buttons
The port select box determines which port is affected by clicking the buttons.
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
CLEAR: Clears the counters for the selected port.

DHCP Relay Statistics



This page provides statistics for DHCP relay.

Server Statistics

Transmit to Server
The number of packets that are relayed from client to server.

Transmit Error
The number of packets that resulted in errors while being sent to clients.

Receive from Server
The number of packets received from server.

Receive Missing Agent Option
The number of packets received without agent information options.

Receive Missing Circuit ID
The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID
The number of packets received with the Remote ID option missing.

Receive Bad Circuit ID
The number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID
The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Transmit to Client
The number of relayed packets from server to client.

Transmit Error
The number of packets that resulted in error while being sent to servers.

Receive from Client
The number of received packets from server.

Receive Agent Option
The number of received packets with relay agent information option.

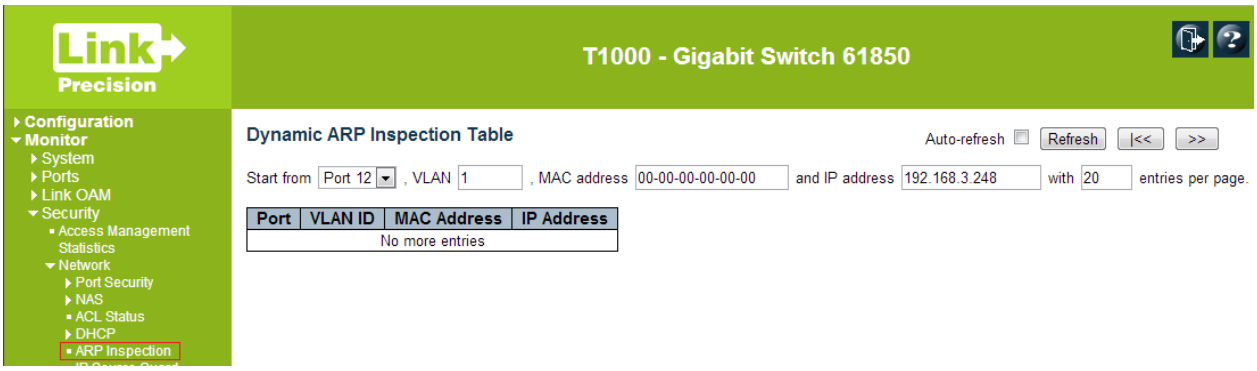
Replace Agent Option
The number of packets which were replaced with relay agent information option.

Keep Agent Option
The number of packets whose relay agent information was retained.

Drop Agent Option
The number of packets that were dropped which were received with relay agent information.

Buttons
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
CLEAR: Clear all statistics.

Dynamic ARP Inspection Table



Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.
The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.
The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

ARP Inspection Table Columns

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the ARP traffic is permitted.

MAC Address

User MAC address of the entry.

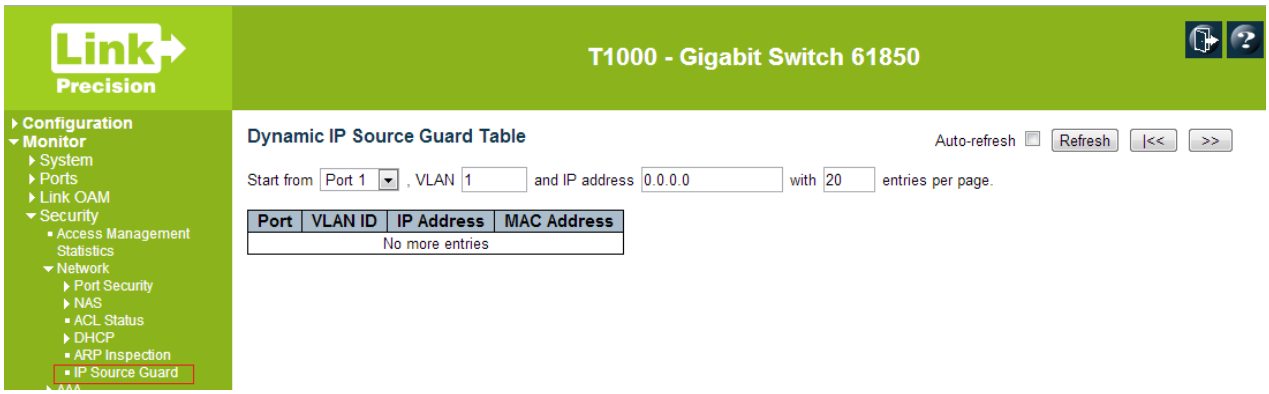
IP Address

User IP address of the entry.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Refreshes the displayed table starting from the input fields.
|<<: Flushes all dynamic entries.
>>: Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

Dynamic IP Source Guard Table



Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

Navigating the IP Source Guard Table

Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table.

The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

IP Source Guard Table Columns

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the IP traffic is permitted.

IP Address

User IP address of the entry.

MAC Address

Source MAC address.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

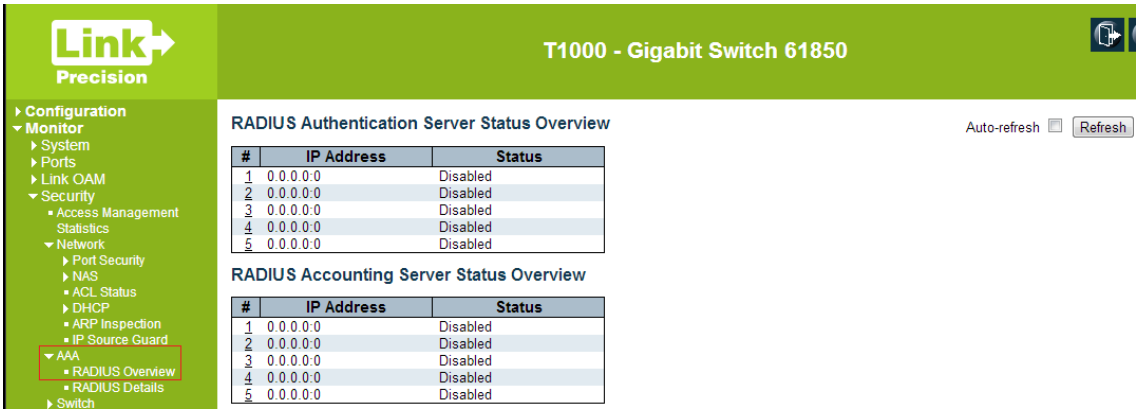
REFRESH: Refreshes the displayed table starting from the input fields.

|<<: Updates the table starting from the first entry in the Dynamic IP Source Guard Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

AAA

RADIUS Authentication Overview



This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.

RADIUS Authentication Servers

#

The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address

The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

Status

The current status of the server. This field takes one of the following values:
Disabled: The server is disabled.
Not Ready: The server is enabled, but IP communication is not yet up and running.
Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Servers

#

The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address

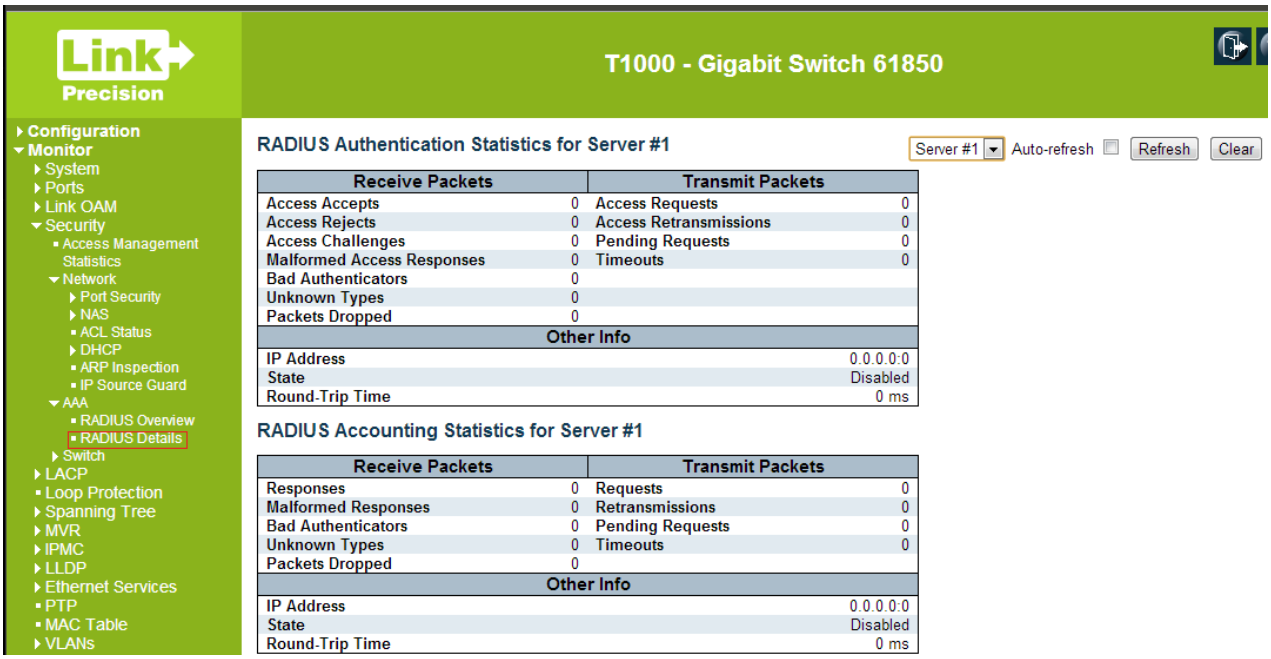
The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

Status

The current status of the server. This field takes one of the following values:
Disabled: The server is disabled.
Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.
Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Authentication Statistics



This page provides detailed statistics for a particular RADIUS server.

RADIUS Authentication Statistics

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.
Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

DIRECTION	NAME	RFC4668 NAME	DESCRIPTION
Rx	Access Accepts	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	Access Rejects	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	Access Challenges	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	Malformed Access Responses	RadiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or

			unknown types are not included as malformed access responses.
Rx	Bad Authenticators	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	Unknown Types	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	Packets Dropped	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	Access Requests	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	Access Retransmissions	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	Pending Requests	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Tx	Timeouts	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Other Info

This section contains information about the state of the server and the latest round-trip time.

NAME	RFC4670 NAME	DESCRIPTION
IP Address	-	IP address and UDP port for the accounting server in question.
State	-	Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB.
Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

DIRECTION	NAME	RFC4668 NAME	DESCRIPTION
Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	Malformed Responses	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
Rx	Bad Authenticators	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from

			the server.
Rx	Unknown Types	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	Packets Dropped	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	Requests	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	Retransmissions	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	Pending Requests	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Tx	Timeouts	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Other Info

This section contains information about the state of the server and the latest round-trip time.

NAME	RFC4670 NAME	DESCRIPTION
IP Address	-	IP address and UDP port for the accounting server in question.
State	-	Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled.

		Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

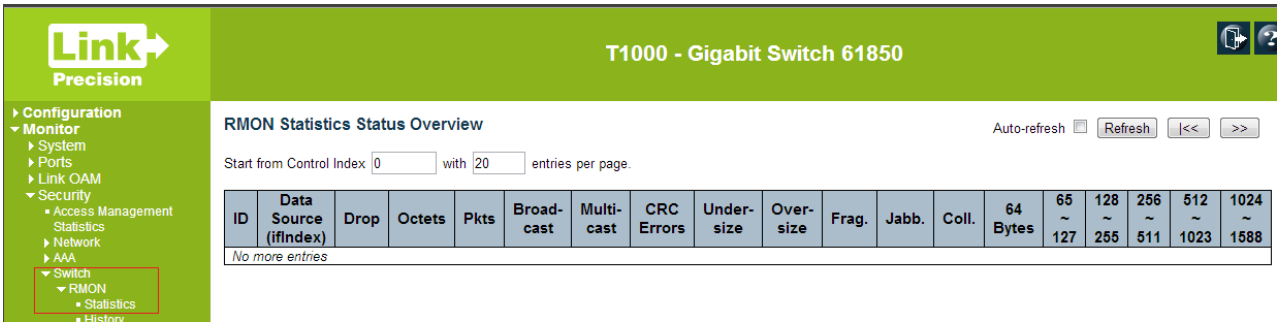
Buttons

The server select box determines which server is affected by clicking the buttons.
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
CLEAR: Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

Switch

RMON

RMON Statistics Overview



This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.
The "Start from Control Index" allows the user to select the starting point in the Statistics table. Clicking the button will update the displayed table starting from that or the next closest Statistics table match. The will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.
The displayed counters are:

ID

Indicates the index of Statistics entry.

Data Source(ifIndex)

The port ID which wants to be monitored.

Drop

The total number of events in which packets were dropped by the probe due to lack of resources.

Octets

The total number of octets of data (including those in bad packets) received on the network.

Pkts

The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broad-cast

The total number of good packets received that were directed to the broadcast address.

Multi-cast

The total number of good packets received that were directed to a multicast address.

CRC Errors
The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 118 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Under-size
The total number of packets received that were less than 64 octets.

Over-size
The total number of packets received that were longer than 118 octets.

Frag.
The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.
The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.
The best estimate of the total number of collisions on this Ethernet segment.

64
The total number of packets (including bad packets) received that were 64 octets in length.

6~127
The total number of packets (including bad packets) received that were between 6 to 127 octets in length.

128~2
The total number of packets (including bad packets) received that were between 128 to 2 octets in length.

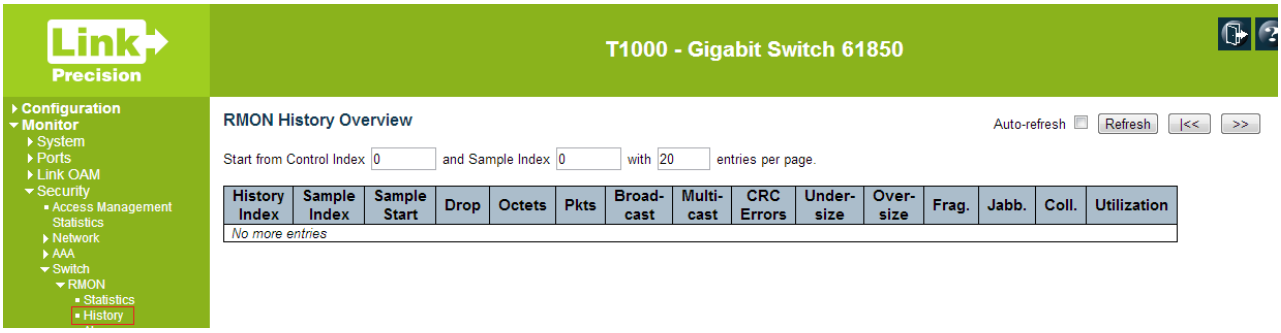
26~11
The total number of packets (including bad packets) received that were between 26 to 11 octets in length.

12~1023
The total number of packets (including bad packets) received that were between 12 to 1023 octets in length.

1024~188
The total number of packets (including bad packets) received that were between 1024 to 188 octets in length.

Buttons
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
|<<: Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.
>>: Updates the table, starting with the entry after the last entry currently displayed.

RMON History Overview



This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.
The "Start from History Index and Sample Index" allows the user to select the starting point in the History table. Clicking the button will update the displayed table starting from that or the next closest History table match.
The will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.
The displayed fields are:

History Index
Indicates the index of History control entry.

Sample Index
Indicates the index of the data entry associated with the control entry.

Sample Start
The value of sysUpTime at the start of the interval over which this sample was measured.

Drop
The total number of events in which packets were dropped by the probe due to lack of resources.

Octets
The total number of octets of data (including those in bad packets) received on the network.

Pkts
The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast
The total number of good packets received that were directed to the broadcast address.

Multicast
The total number of good packets received that were directed to a multicast address.

CRCErrors
The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 118 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with

an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Undersize
The total number of packets received that were less than 64 octets.

Oversize
The total number of packets received that were longer than 118 octets.

Frag.
The number of frames which size is less than 64 octets received with invalid CRC.

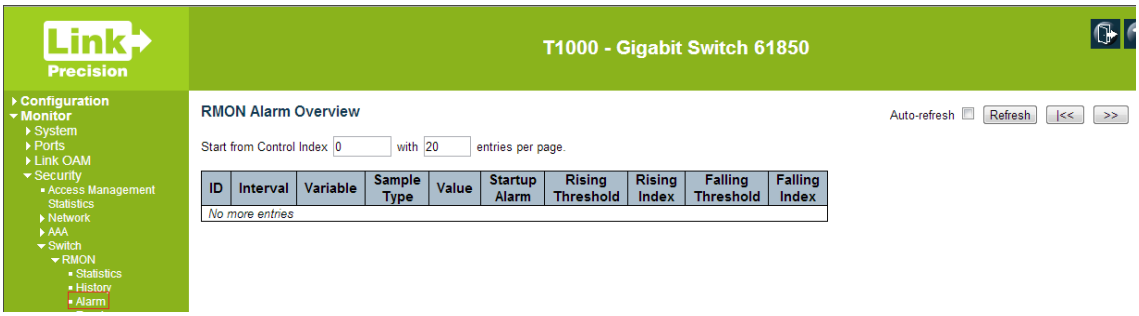
Jabb.
The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.
The best estimate of the total number of collisions on this Ethernet segment.

Utilization
The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
|<<: Updates the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index
>>: Updates the table, starting with the entry after the last entry currently displayed.

RMON Alarm Overview



This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.
The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the button will update the displayed table starting from that or the next closest Alarm table match. The will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.
The displayed fields are:

ID

Indicates the index of Alarm control entry.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable

Indicates the particular variable to be sampled

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the thresholds.

Value

The value of the statistic during the last sampling period.

Startup Alarm

The alarm that may be sent when this entry is first set to valid.

Rising Threshold

Rising threshold value.

Rising Index

Rising event index.

Falling Threshold

Falling threshold value.

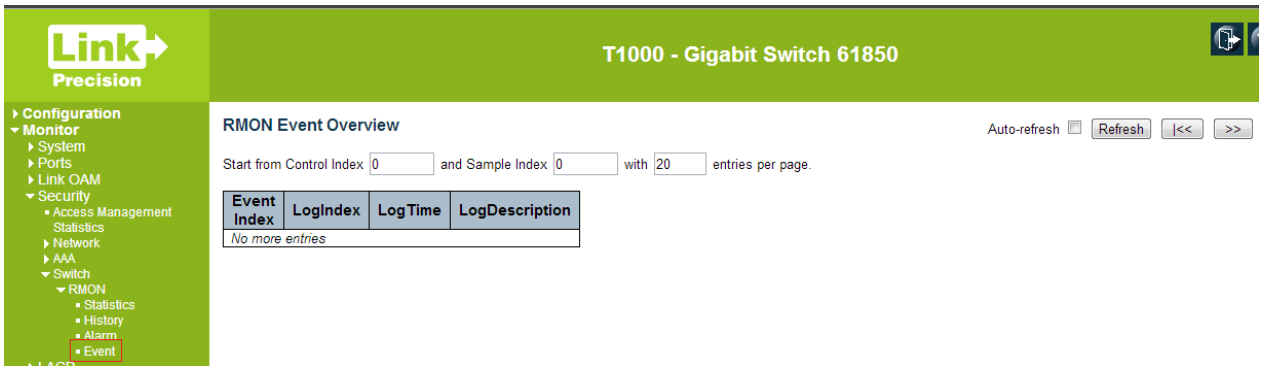
Falling Index

Falling event index.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
|<<: Updates the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index
>>: Updates the table, starting with the entry after the last entry currently displayed.

RMON Event Overview



This page provides an overview of RMON Event table entries.Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table table.
The "Start from Event Index and Log Index" allows the user to select the starting point in the Event table. Clicking the button will update the displayed table starting from that or the next closest Event table match.
The will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.
The displayed fields are:

Event Index

Indicates the index of the event entry.

Log Index

Indicates the index of the log entry.

LogTIme

Indicates Event log time

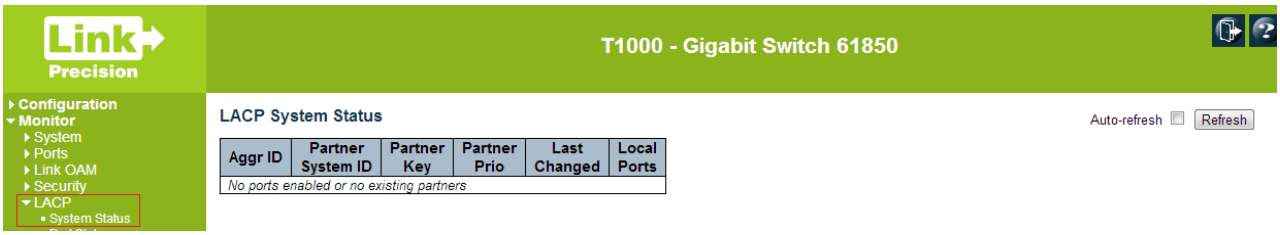
LogDescription

Indicates the Event description.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
: Click to refresh the page immediately.
: Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.
: Updates the table, starting with the entry after the last entry currently displayed.

LACP



LACP System Status

This page provides a status overview for all LACP instances.

Aggr ID

The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'

Partner System ID

The system ID (MAC address) of the aggregation partner.

Partner Key

The Key that the partner has assigned to this aggregation ID.

Last changed

The time since this aggregation changed.

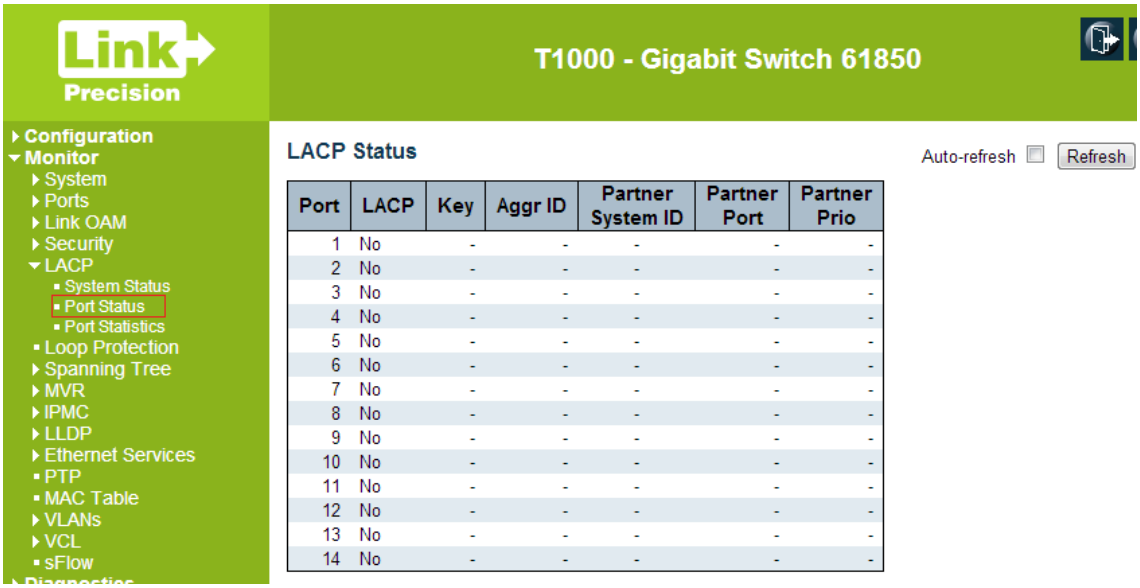
Local Ports

Shows which ports are a part of this aggregation for this switch.

Buttons

REFRESH: Click to refresh the page immediately.
AUTO-REFRESH: Automatic refresh occurs every 3 seconds.

LACP Port Status



This page provides a status overview for LACP status for all ports.

Port

The switch port number.

LACP

'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.

Key

The key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID

The Aggregation ID assigned to this aggregation group.

Partner System ID

The partner's System ID (MAC address).

Partner Port

The partner's port number connected to this port.

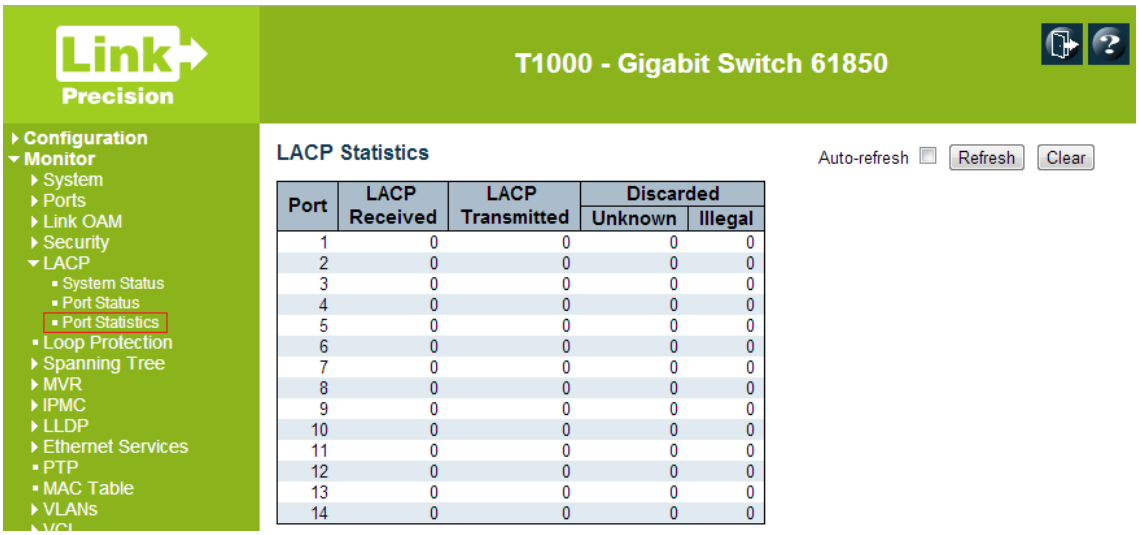
Partner Prio

The partner's port priority.

Buttons

REFRESH: Click to refresh the page immediately.
AUTO-REFRESH: Automatic refresh occurs every 3 seconds.

LACP statistics



This page provides an overview for LACP statistics for all ports.

Port

The switch port number.

LACP Received

Shows how many LACP frames have been received at each port.

LACP Transmitted

Shows how many LACP frames have been sent from each port.

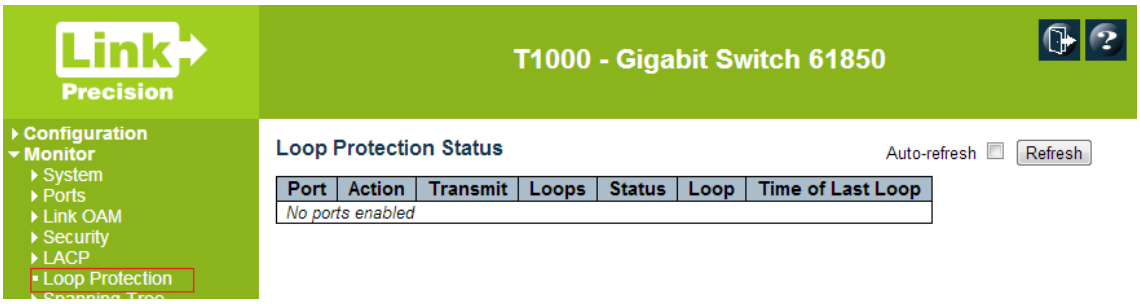
Discarded

Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

AUTO-REFRESH: Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
CLEAR: Clears the counters for all ports.

Loop Protection



Loop Protection Status

This page displays the loop protection port status the ports of the switch.
Loop protection port status is:

Port
The switch port number of the logical port.

Action
The currently configured port action.

Transmit
The currently configured port transmit mode.

Loops
The number of loops detected on this port.

Status
The current loop protection status of the port.

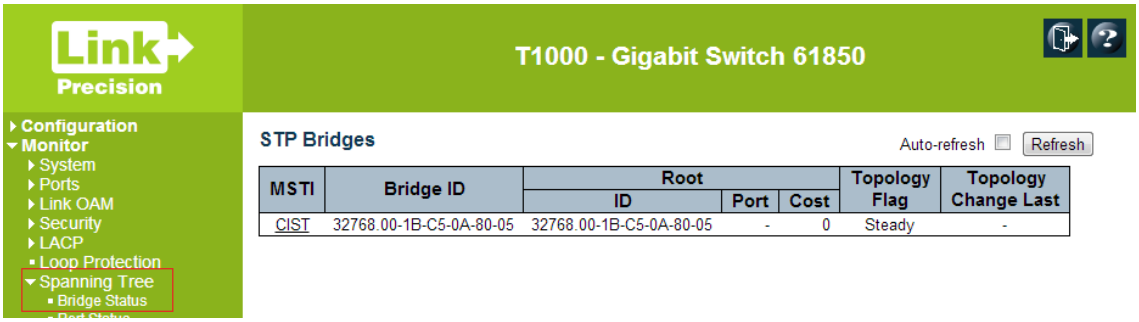
Loop
Whether a loop is currently detected on the port.

Time of Last Loop
The time of the last loop event detected.

Buttons
REFRESH: Click to refresh the page immediately.
AUTO-REFRESH: Check this box to enable an automatic refresh of the page at regular intervals.

Spanning Tree

STP Bridge Status



This page provides a status overview of all STP bridge instances.
The displayed table contains a row for each STP bridge instance, where the column displays the following information:

MSTI

The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

Bridge ID

The Bridge ID of this Bridge instance.

Root ID

The Bridge ID of the currently elected root bridge.

Root Port

The switch port currently assigned the root port role.

Root Cost

Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag

The current state of the Topology Change Flag of this Bridge instance.

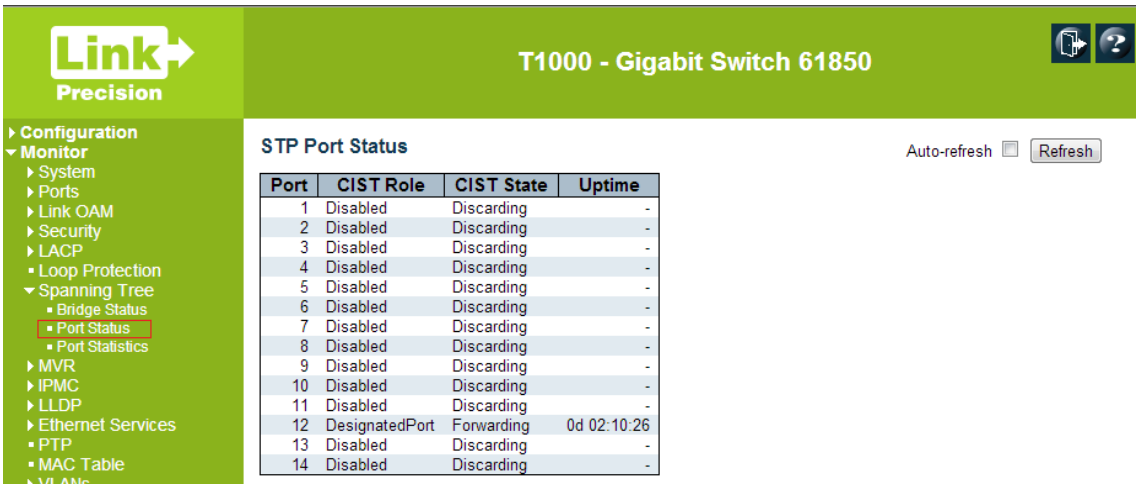
Topology Change Last

The time since last Topology Change occurred.

Buttons

REFRESH: Click to refresh the page immediately.
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

STP Port Status



This page displays the STP CIST port status for physical ports of the switch.
STP port status is:

Port

The switch port number of the logical STP port.

CIST Role

The current STP port role of the CIST port. The port role can be one of the following values: AlternatePortBackupPort RootPort DesignatedPortDisabled.

CIST State

The current STP port state of the CIST port. The port state can be one of the following values: DiscardingLearning Forwarding.

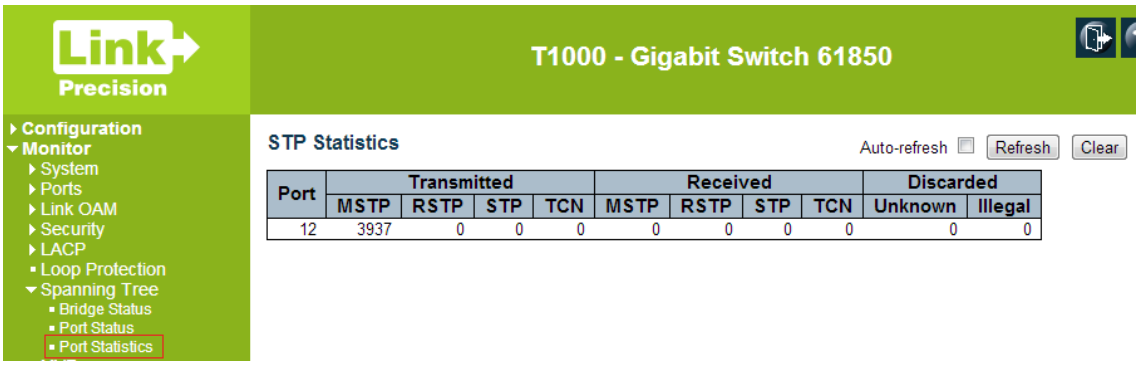
Uptime

The time since the bridge port was last initialized.

Buttons

REFRESH: Click to refresh the page immediately.
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

STP Port Statistics



This page displays the STP port statistics counters of bridge ports in the switch.
The STP port statistics counters are:

Port

The switch port number of the logical STP port.

MSTP

The number of MSTP BPDU's received/transmitted on the port.

RSTP

The number of RSTP BPDU's received/transmitted on the port.

STP

The number of legacy STP Configuration BPDU's received/transmitted on the port.

TCN

The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.

Discarded Unknown

The number of unknown Spanning Tree BPDU's received (and discarded) on the port.

Discarded Illegal

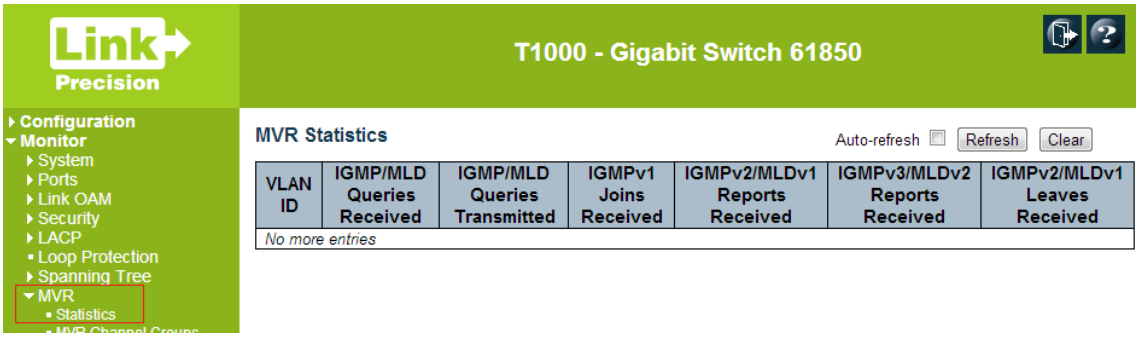
The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons

REFRESH: Click to refresh the page immediately.
RESET: Click to reset the counters.
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

MVR

MVR Statistics Table



This page provides MVR Statistics information.

VLAN ID

The Multicast VLAN ID.

IGMP/MLD Queries Received

The number of Received Queries for IGMP and MLD, respectively.

IGMP/MLD Queries Transmitted

The number of Transmitted Queries for IGMP and MLD, respectively.

IGMPv1 Joins Received

The number of Received IGMPv1 Join's.

IGMPv2/MLDv1 Report's Received

The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.

IGMPv3/MLDv2 Report's Received

The number of Received IGMPv1 Join's and MLDv2 Report's, respectively.

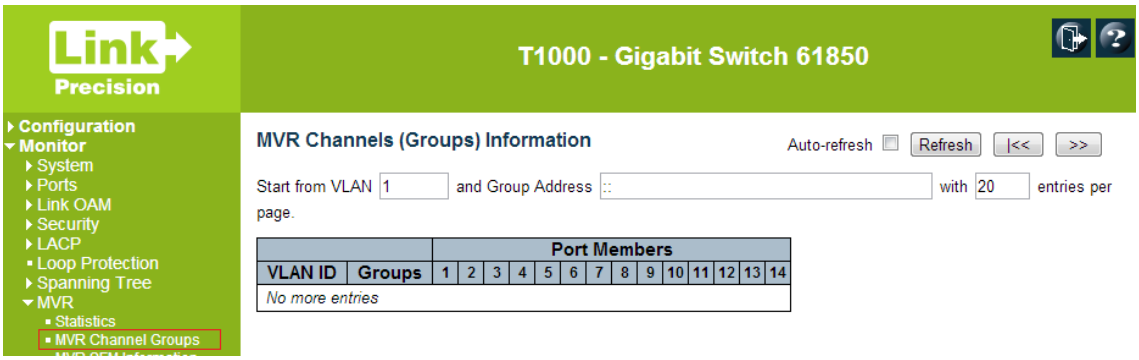
IGMPv2/MLDv1 Leave's Received

The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

Buttons

AUTO-REFRESH : Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
CLEAR: Clears all Statistics counters.

MVR Channels Groups Information Table



Entries in the MVR Channels (Groups) Information Table are shown on this page. The MVR Channels (Groups) Information Table is sorted first by VLAN ID, and then by group.

Navigating the MVR Channels (Groups) Information Table

Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information Table.
The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. Clicking the button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.
The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

MVR Channels (Groups) Information Table Columns

VLAN ID

VLAN ID of the group.

Groups

Group ID of the group displayed.

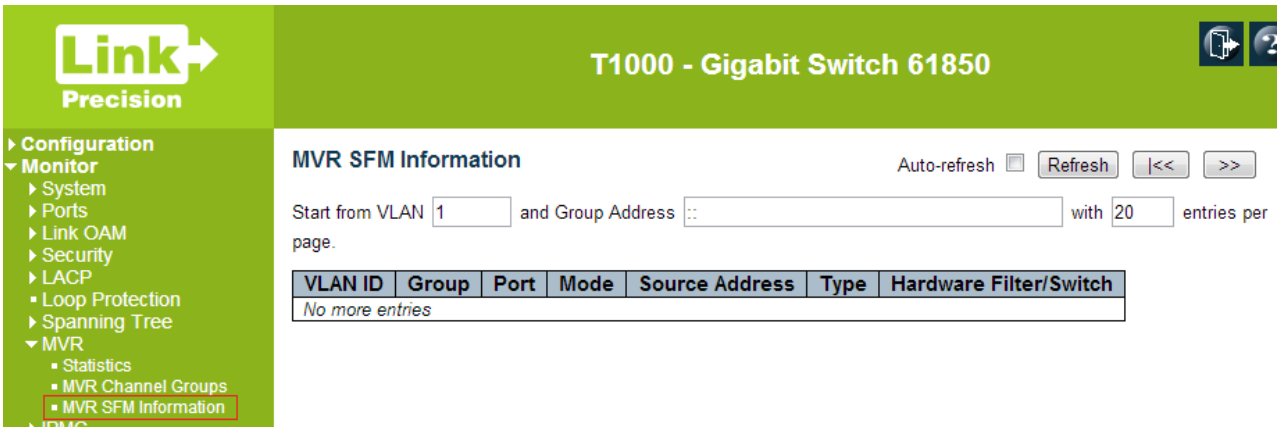
Port Members

Ports under this group.

Buttons

AUTO-REFRESH : Automatic refresh occurs every 3 seconds.
REFRESH: Refreshes the displayed table starting from the input fields.
|<<: Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.
>>: Updates the table, starting with the entry after the last entry currently displayed.

MVR SFM Information Table



Entries in the MVR SFM Information Table are shown on this page. The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Navigating the MVR SFM Information Table

Each page shows up to 99 entries from the MVR SFM Information Table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table.
The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR SFM Information Table. Clicking the button will update the displayed table starting from that or the closest next MVR SFM Information Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.
The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

MVR SFM Information Table Columns

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

Switch port number.

Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address

IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field.

Type
Indicates the Type. It can be either Allow or Deny.

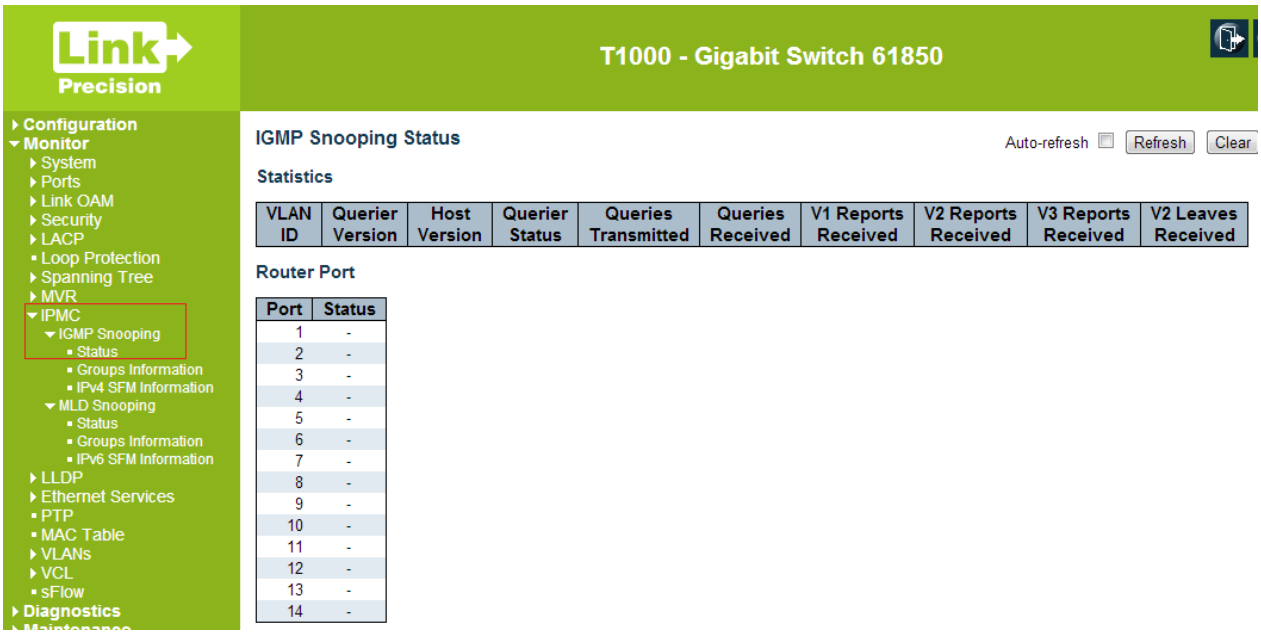
Hardware Filter/Switch
Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

Buttons
AUTO-REFRESH : Automatic refresh occurs every 3 seconds.
REFRESH: Refreshes the displayed table starting from the input fields.
|<<: Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.
>>: Updates the table, starting with the entry after the last entry currently displayed.

IPMC

IGMP Snooping

IGMP Snooping Status



This page provides IGMP Snooping status.

VLAN ID

The VLAN ID of the entry.

Querier Version

Working Querier Version currently.

Host Version

Working Host Version currently.

Querier Status

Shows the Querier status is "ACTIVE" or "IDLE".
"DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted

The number of Transmitted Queries.

Queries Received

The number of Received Queries.

V1 Reports Received
The number of Received V1 Reports.

V2 Reports Received
The number of Received V2 Reports.

V3 Reports Received
The number of Received V3 Reports.

V2 Leaves Received
The number of Received V2 Leaves.

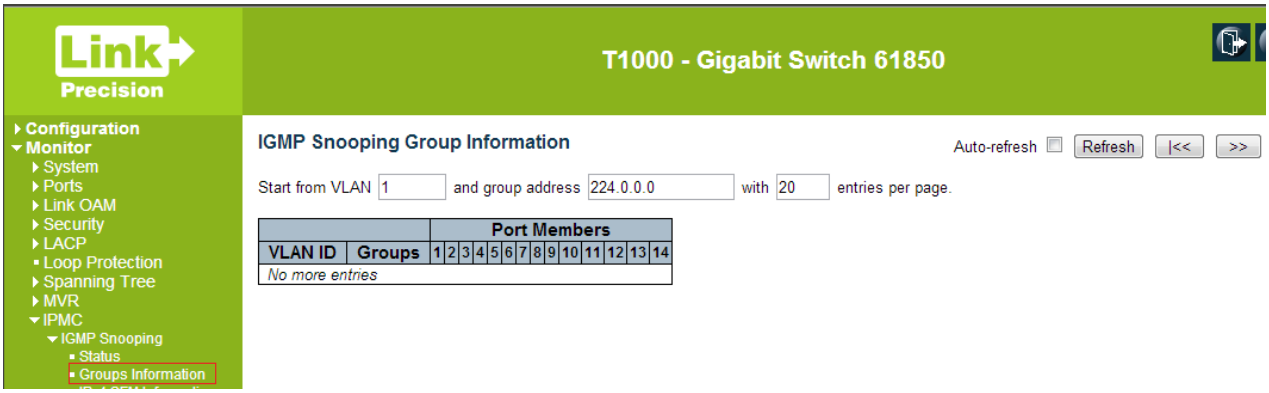
Router Port
Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.
Static denotes the specific port is configured to be a router port.
Dynamic denotes the specific port is learnt to be a router port.
Both denote the specific port is configured or learnt to be a router port.

Port
Switch port number.

Status
Indicate whether specific port is a router port or not.

Buttons
AUTO-REFRESH : Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
CLEAR: Clears all Statistics counters.

IGMP Group Information Table



Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.

Navigating the IGMP Group Table

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP Group Table. Clicking the button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

IGMP Group Table Columns

VLAN ID

VLAN ID of the group.

Groups

Group address of the group displayed.

Port Members

Ports under this group.

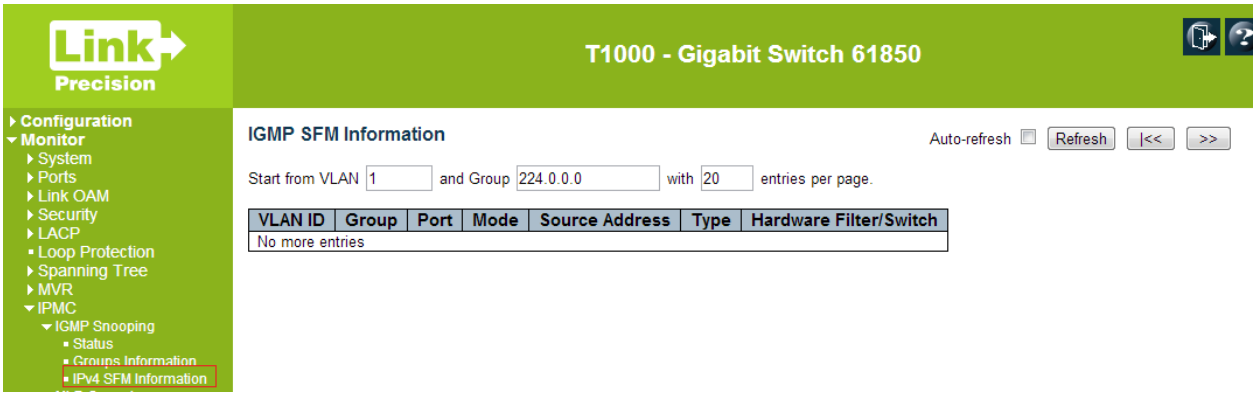
Buttons

AUTO-REFRESH: Automatic refresh occurs every 3 seconds.

REFRESH: Click to refresh the page immediately.

CLEAR: Clears all Statistics counters.

IGMP SFM Information Table



Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Navigating the IGMP SFM Information Table

Each page shows up to 99 entries from the IGMP SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP SFM Information Table. Clicking the button will update the displayed table starting from that or the closest next IGMP SFM Information Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

IGMP SFM Information Table Columns

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

Switch port number.

Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address

IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type

Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch

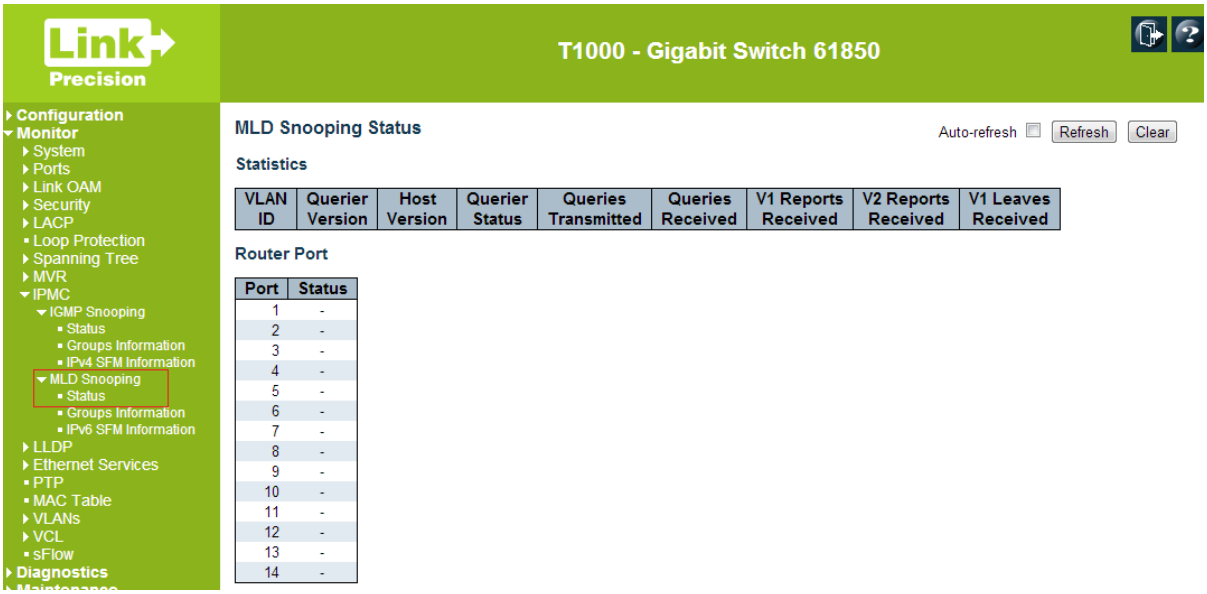
Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

Buttons

AUTO-REFRESH: Automatic refresh occurs every 3 seconds.
REFRESH: Refreshes the displayed table starting from the input fields.
|<<: Updates the table starting from the first entry in the IGMP SFM Information Table.
>>: Updates the table, starting with the entry after the last entry currently displayed.

MLD Snooping

MLD Snooping Status



This page provides MLD Snooping status.

VLAN ID

The VLAN ID of the entry.

Querier Version

Working Querier Version currently.

Host Version

Working Host Version currently.

Querier Status

Shows the Querier status is "ACTIVE" or "IDLE".
"DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted

The number of Transmitted Queries.

Queries Received

The number of Received Queries.

V1 Reports Received

The number of Received V1 Reports.

V2 Reports Received

The number of Received V2 Reports.

V1 Leaves Received

The number of Received V1 Leaves.

Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.
Static denotes the specific port is configured to be a router port.
Dynamic denotes the specific port is learnt to be a router port.
Both denote the specific port is configured or learnt to be a router port.

Port

Switch port number.

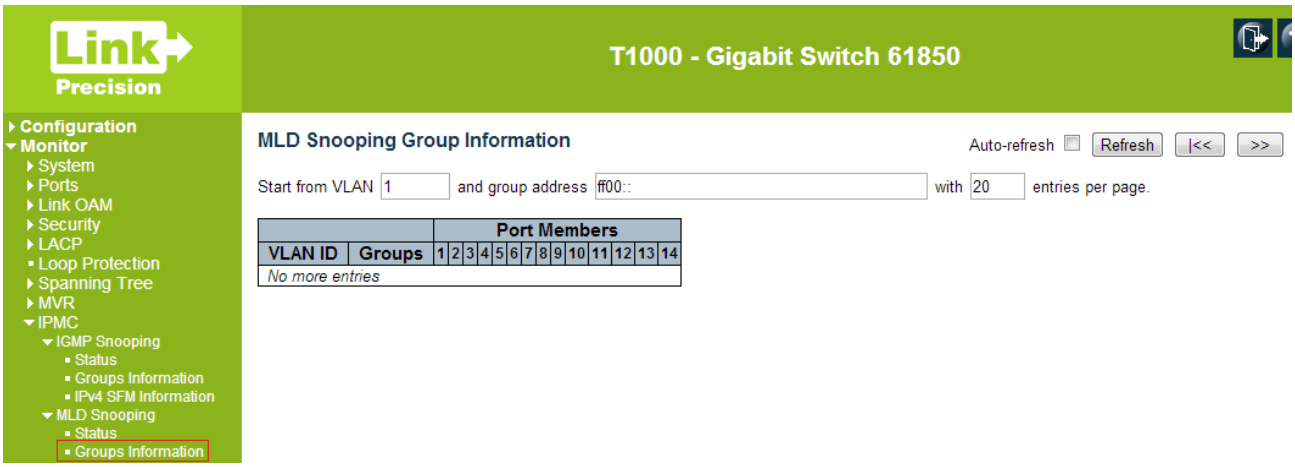
Status

Indicate whether specific port is a router port or not.

Buttons

AUTO-REFRESH: Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
CLEAR: Clears all Statistics counters.

MLD Group Table



Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group.

Navigating the MLD Group Table

Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. Clicking the button will update the displayed table starting from that or the closest next MLD Group Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

MLD Group Table Columns

VLAN ID

VLAN ID of the group.

Groups

Group address of the group displayed.

Port Members

Ports under this group.

Buttons

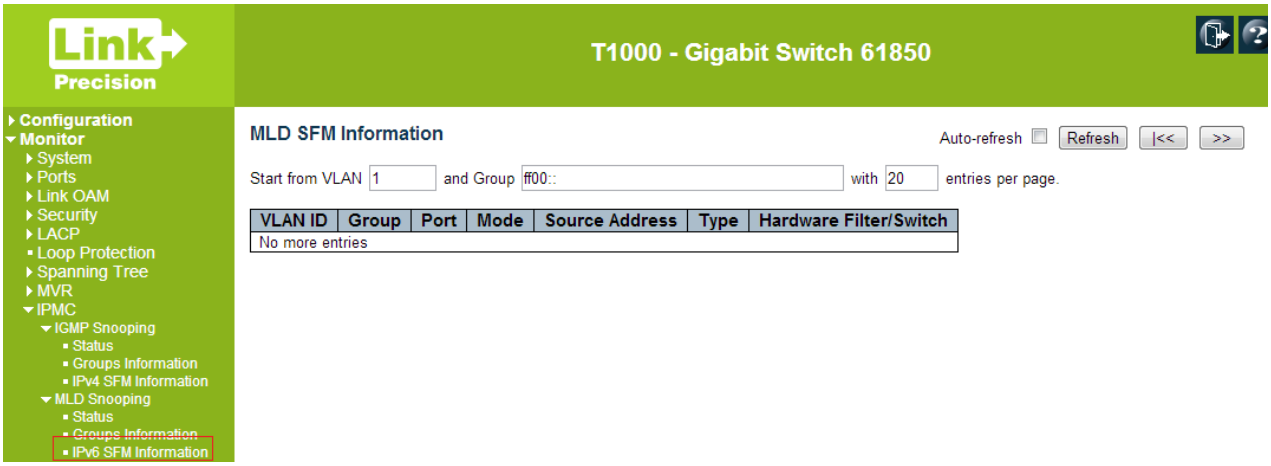
AUTO-REFRESH: Automatic refresh occurs every 3 seconds.

REFRESH: Refreshes the displayed table starting from the input fields.

|<<: Updates the table starting from the first entry in the IGMP SFM Information Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

MLD SFM Information Table



Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Navigating the MLD SFM Information Table

Each page shows up to 99 entries from the MLD SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD SFM Information Table. Clicking the button will update the displayed table starting from that or the closest next MLD SFM Information Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

MLD SFM Information Table Columns

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

Switch port number.

Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address

IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type

Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch

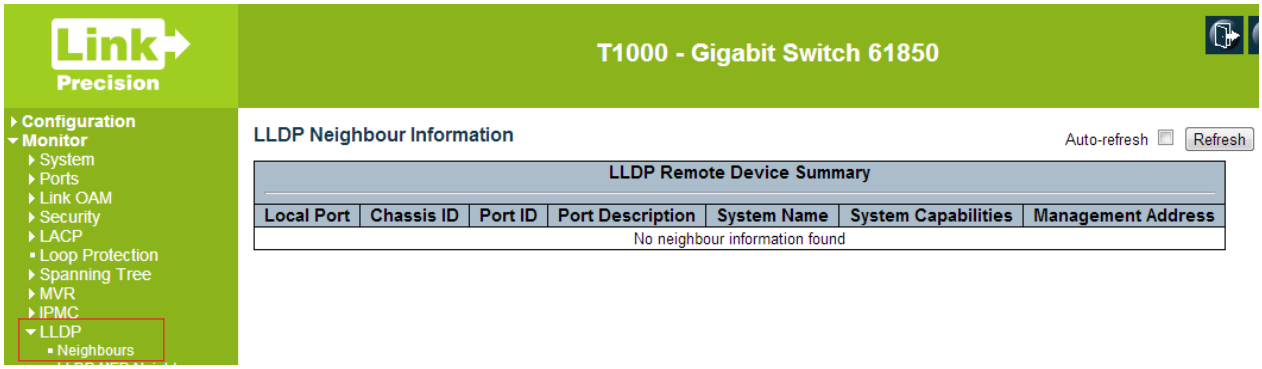
Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Buttons

AUTO-REFRESH: Automatic refresh occurs every 3 seconds.
REFRESH: Refreshes the displayed table starting from the input fields.
|<<: Updates the table starting from the first entry in the IGMP SFM Information Table.
>>: Updates the table, starting with the entry after the last entry currently displayed.

LLDP

LLDP Neighbour



This page provides a status overview for all LLDP neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. The columns hold the following information:

Local Port

The port on which the LLDP frame was received.

Chassis ID

The Chassis ID is the identification of the neighbour's LLDP frames.

Port ID

The Port ID is the identification of the neighbour port.

Port Description

Port Description is the port description advertised by the neighbour unit.

System Name

System Name is the name advertised by the neighbour unit.

System Capabilities

System Capabilities describes the neighbour unit's capabilities. The possible capabilities are:
1. Other
2. Repeater
3. Bridge
4. WLAN Access Point
. Router
6. Telephone
7. DOCSIS cable device
8. Station only
9. Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

Management Address

Management Address is the neighbour unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbour's IP address.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page.

LLDP Media

This page provides a status overview of all LLDP-MEDneighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. This function applies to VoIP devices which support LLDP-MED. The columns hold the following information:

Port

The port on which the LLDP frame was received.

Device Type

LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Device Definition

LLDP-MED Network Connectivity Devices, as defined in TIA-107, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:
1. LAN Switch/Router
2. IEEE 802.1 Bridge
3. IEEE 802.3 Repeater (included for historical reasons)
4. IEEE 802.11 Wireless Access Point
. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-107 and can relay IEEE 802 frames via any method.

LLDP-MED Endpoint Device Definition

LLDP-MED Endpoint Devices, as defined in TIA-107, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.
Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.
Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-107 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-107 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

LLDP-MED Generic Endpoint (Class I)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-107, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication

Controllers, other communication related servers, or any device requiring basic services as defined in TIA-107.
Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.
Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.
Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

LLDP-MED Capabilities

LLDP-MED Capabilities describes the neighbour unit's LLDP-MED capabilities. The possible capabilities are:
1. LLDP-MED capabilities
2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE
. Extended Power via MDI - PD
6. Inventory
7. Reserved

Application Type

Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.
1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.
3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.
. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.
6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.

Policy

Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown
Unknown: The network policy for the specified application type is currently unknown.
Defined: The network policy is defined.

TAG

TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.
Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.
Tagged: The device is using the IEEE 802.1Q tagged frame format.

VLAN ID

VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

Priority

Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).

DSCP

DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

Auto-negotiation

Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.

Auto-negotiation status

Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

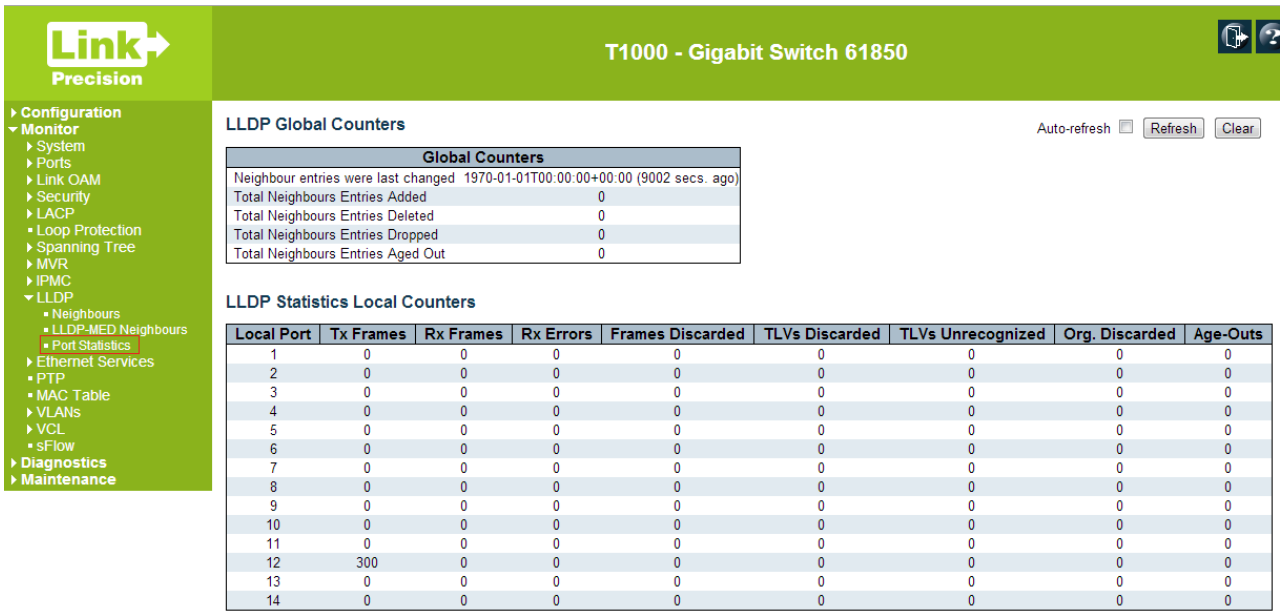
Auto-negotiation Capabilities

Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page.

LLDP Statistics


Link Precision
T1000 - Gigabit Switch 61850
Configuration
Monitor
System
Ports
Link OAM
Security
LACP
Loop Protection
Spanning Tree
MVR
IPMC
LLDP
Neighbours
LLDP-MED Neighbours
Port Statistics
Ethernet Services
PTP
MAC Table
VLANs
VCL
sFlow
Diagnostics
Maintenance
LLDP Global Counters
Auto-refresh
Refresh
Clear
Global Counters
Neighbour entries were last changed 1970-01-01T00:00:00+00:00 (9002 secs. ago)
Total Neighbours Entries Added 0
Total Neighbours Entries Deleted 0
Total Neighbours Entries Dropped 0
Total Neighbours Entries Aged Out 0
LLDP Statistics Local Counters
Local Port | Tx Frames | Rx Frames | Rx Errors | Frames Discarded | TLVs Discarded | TLVs Unrecognized | Org. Discarded | Age-Outs
1 0 0 0 0 0 0 0 0
2 0 0 0 0 0 0 0 0
3 0 0 0 0 0 0 0 0
4 0 0 0 0 0 0 0 0
5 0 0 0 0 0 0 0 0
6 0 0 0 0 0 0 0 0
7 0 0 0 0 0 0 0 0
8 0 0 0 0 0 0 0 0
9 0 0 0 0 0 0 0 0
10 0 0 0 0 0 0 0 0
11 0 0 0 0 0 0 0 0
12 300 0 0 0 0 0 0 0
13 0 0 0 0 0 0 0 0
14 0 0 0 0 0 0 0 0

This page provides an overview of all LLDP traffic.
Two types of counters are shown. Global counters are counters that refer to the whole switch, while local countersrefer to per port counters for the currently selected switch.

Global Counters

Neighbour entries were last changed

Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbours Entries Added

Shows the number of new entries added since switch reboot.

Total Neighbours Entries Deleted

Shows the number of new entries deleted since switch reboot.

Total Neighbours Entries Dropped

Shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbours Entries Aged Out

Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

Local Port

The port on which LLDP frames are received or transmitted.

Tx Frames

The number of LLDP frames transmitted on the port.

Rx Frames
The number of LLDP frames received on the port.

Rx Errors
The number of received LLDP frames containing some kind of error.

Frames Discarded
If a LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, anLLDP shutdown frame is received, or when the entry ages out.

TLVs Discarded
Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized
The number of well-formed TLVs, but with an unknown type value.

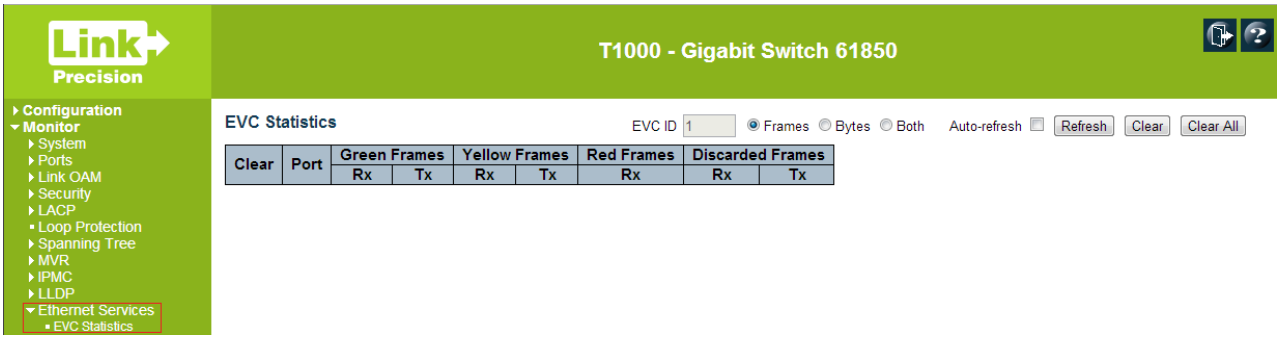
Org. Discarded
If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.

Age-Outs
Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDPframe is received within the age out time, the LLDPinformation is removed, and the Age-Out counter is incremented.

Buttons
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page.
CLEAR: Clears the local counters. All counters (includingglobal counters) are cleared upon reboot.

Ethernet Services

EVC Statistics



This page provides NNI port traffic statistics for the selected EVC. It also shows counters for UNI ports of ECEs mapping to the EVC.

Clear

This box is used to mark a port for clearance in next Clear operation.

Port

The UNI/NNI port for the EVC.

Rx Green

The number of green received.

Tx Green

The number of green transmitted.

Rx Yellow

The number of yellow received.

Tx Yellow

The number of yellow transmitted.

Rx Red

The number of red received.

Rx Discarded

The number of discarded in the ingress queue system.

Tx Discarded

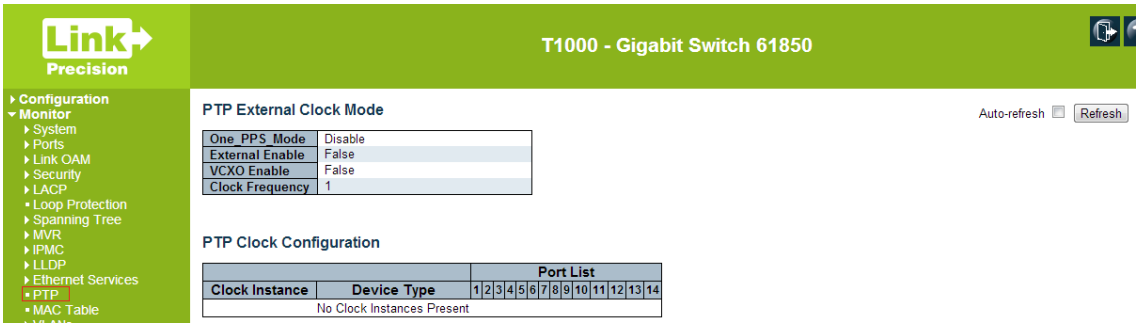
The number of discarded in the egress queue system.

Buttons

FRAMES: Show frames statistics only.
BYTES: Show bytes statistics only.
BOTH: Show both frames and bytes statistics.
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.
CLEAR: Clears the counters for selected ports.
CLEAR ALL: Clears the counters for all ports.

PTP

PTP Clock Monitor



This page allows the user to inspect the current PTP clock settings.

One_pps_mode

Shows the current One_pps_mode configured.
1. Output : Enable the 1 pps clock output
2. Input : Enable the 1 pps clock input
3. Disable : Disable the 1 pps clock in/out-put

External Enable

Shows the current External clock output configuration.
1. True : Enable the external clock output
2. False : Disable the external clock output

VCXO_Enable

Shows the current VCXO rate adjustment configuration.
1. True : Enable the external VCXO rate adjustment
2. False : Disable the external VCXO rate adjustment

Clock Frequency

Shows the current clock frequency used by the External Clock.
The possible range of values are 1 - 2000000 (1 - 2MHz)

PTP Clock Description

Clock Instance

Indicates the Instance of a particular Clock Instance [0..3].
Click on the Clock Instance number to monitor the Clock details.

Device Type

Indicates the Type of the Clock Instance. There are five Device Types.
1. Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.

2. P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.
3. E2e Transp - Clock's Device Type is End to End Transparent Clock.
4. Master Only - Clock's Device Type is Master Only.
. Slave Only - Clock's Device Type is Slave Only.

Port List

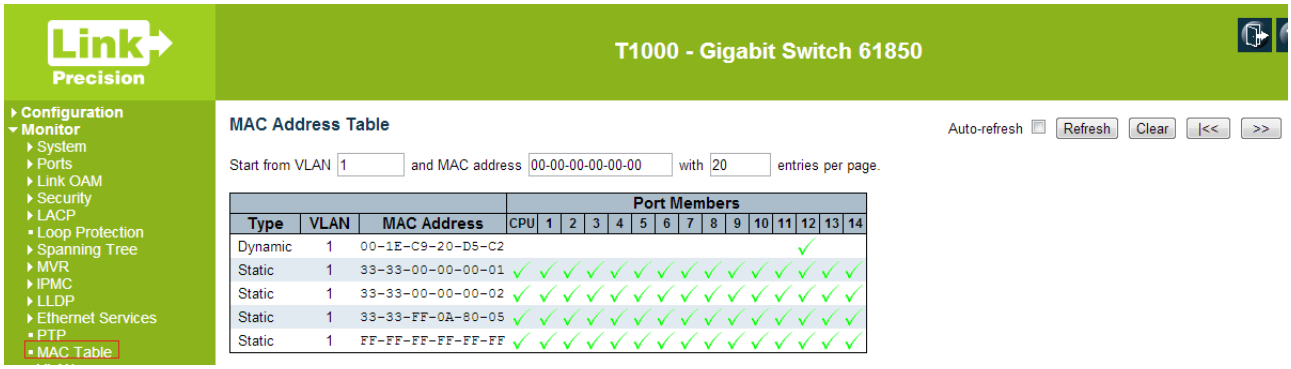
Shows the ports configured for that Clock Instance.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.

MAC Table

Dynamic MAC Table



Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.
The "Start from MAC address" and "VLAN" input fields allow the user to select the starting point in the MAC Table. Clicking the button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.
The will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

MAC Table Columns

Switch (stack only)

The stack unit where the entry is learned.

Type

Indicates whether the entry is a static or a dynamic entry.

MAC address

The MAC address of the entry.

VLAN

The VLAN ID of the entry.

Port Members

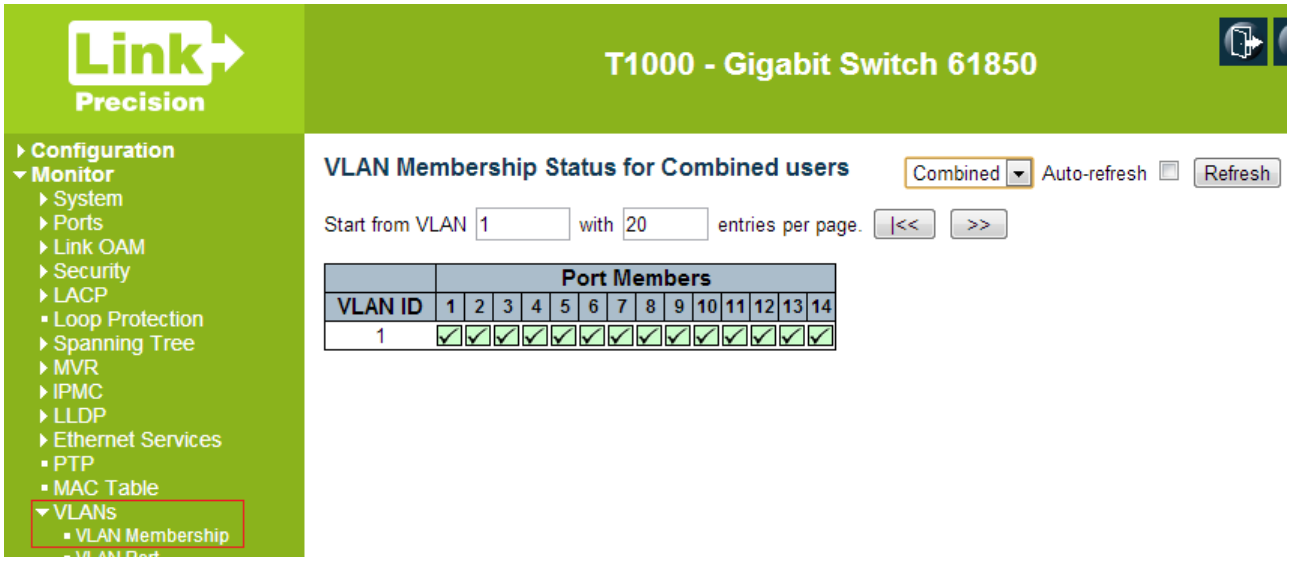
The ports that are members of the entry.

Buttons

AUTO-REFRESH: Automatic refresh occurs every 3 seconds.
REFRESH: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.
CLEAR: Flushes all dynamic entries.
|<<: Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.
>>: Updates the table, starting with the entry after the last entry currently displayed.

VLANs

VLAN Membership Status



This page provides an overview of membership status of VLAN users.

VLAN USER

VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently we support the following VLAN user types:
CLI/Web/SNMP : These are referred to as static.
NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.
MVR : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.
MSTP : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

VLAN ID

VLAN ID for which the Port members are displayed.

Port Members

A row of check boxes for each port is displayed for each VLAN ID.
If a port is included in a VLAN, an image will be displayed.
If a port is included in a Forbidden port list, an image will be displayed.
If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as .

VLAN Membership

The VLAN Membership Status Page shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When ALL VLAN Users are selected, it shall show this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Navigating the VLAN Monitor page

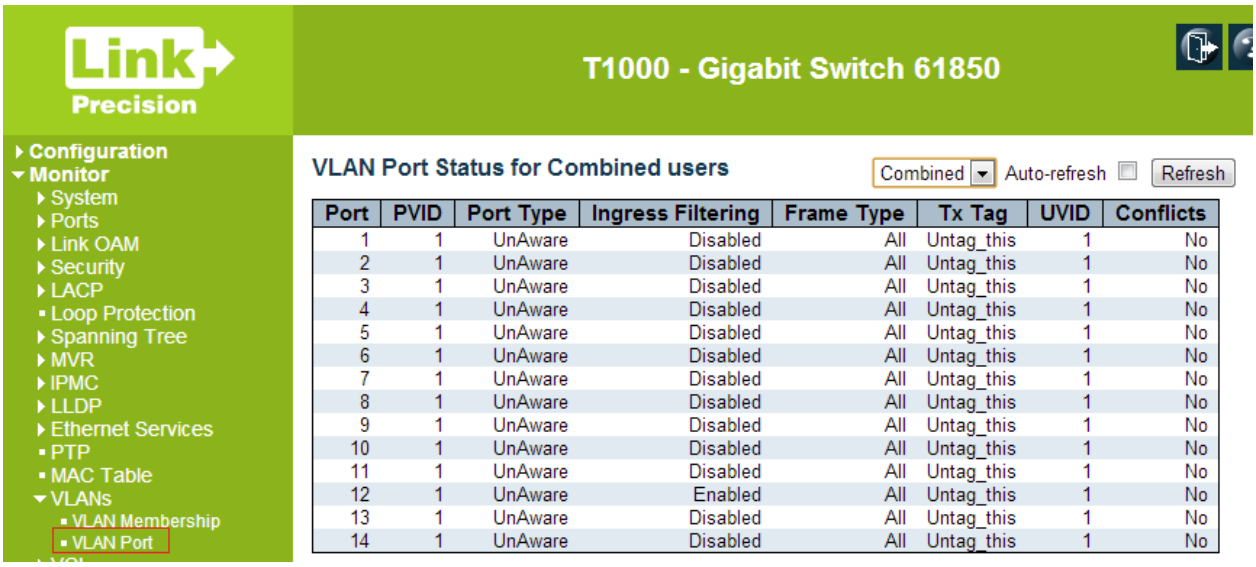
Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the closest next VLAN Table match. The will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

Buttons

: Select VLAN Users from this drop down list.

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.

VLAN Port Status


Link Precision
T1000 - Gigabit Switch 61850
Configuration
Monitor
System
Ports
Link OAM
Security
LACP
Loop Protection
Spanning Tree
MVR
IPMC
LLDP
Ethernet Services
PTP
MAC Table
VLANs
VLAN Membership
VLAN Port
VLAN Port Status for Combined users
Combined
Auto-refresh
Refresh
Port PVID Port Type Ingress Filtering Frame Type Tx Tag UVID Conflicts
1 1 UnAware Disabled All Untag_this 1 No
2 1 UnAware Disabled All Untag_this 1 No
3 1 UnAware Disabled All Untag_this 1 No
4 1 UnAware Disabled All Untag_this 1 No
5 1 UnAware Disabled All Untag_this 1 No
6 1 UnAware Disabled All Untag_this 1 No
7 1 UnAware Disabled All Untag_this 1 No
8 1 UnAware Disabled All Untag_this 1 No
9 1 UnAware Disabled All Untag_this 1 No
10 1 UnAware Disabled All Untag_this 1 No
11 1 UnAware Disabled All Untag_this 1 No
12 1 UnAware Enabled All Untag_this 1 No
13 1 UnAware Disabled All Untag_this 1 No
14 1 UnAware Disabled All Untag_this 1 No

This page provides VLAN Port Status.

VLAN USER

VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN User types:
CLI/Web/SNMP : These are referred to as static.
NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.
MVR : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.
MSTP : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

Port

The logical port for the settings contained in the same row.

PVID

Shows the VLAN identifier for that port. The allowed values are 1 through 409. The default value is 1.

Port Type

Shows the Port Type. Port type can be any of Unaware, C-port, S-port, Custom S-port.
If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.
C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.

Ingress Filtering

Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

Frame Type

Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.

Tx Tag

Shows egress filtering frame status whether tagged or untagged.

UVID

Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behaviour at the egress side.

Conflicts

Shows status of Conflicts whether exists or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:
Functional Conflicts between features.
Conflicts due to hardware limitation.
Direct conflict between user modules.

Buttons

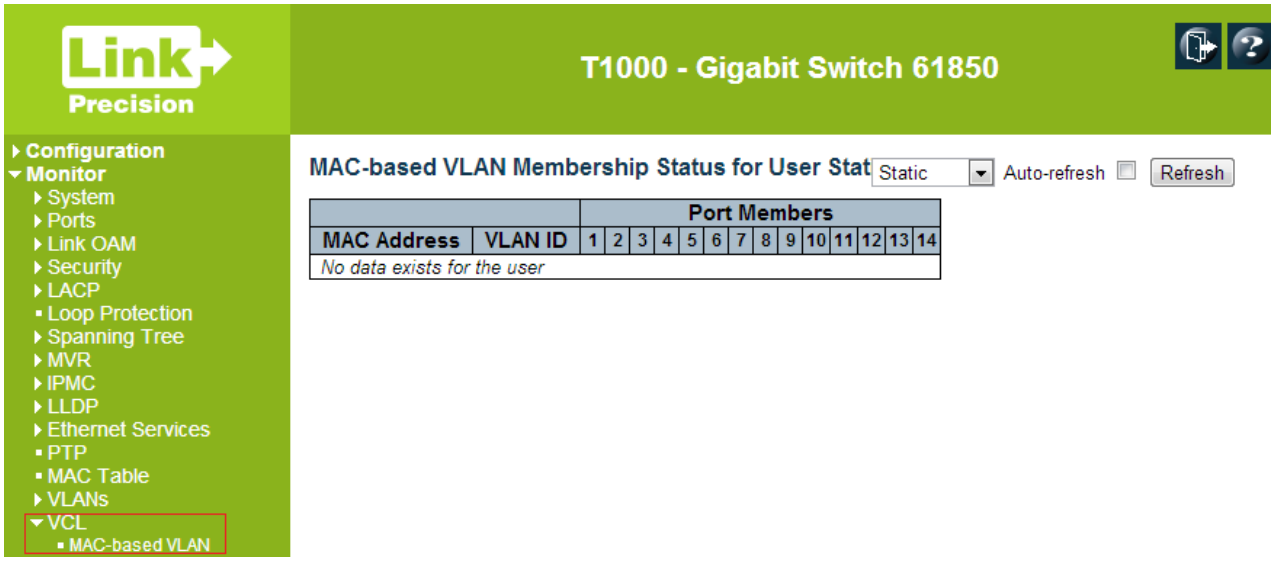
: Select VLAN Users from this drop down list.

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page immediately.

VCL

VCL MAC-Based VLAN Status

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently we support following VLAN User types:
CLI/Web/SNMP : These are referred to as static.



NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

MAC Address

Indicates the MAC address.

VLAN ID

Indicates the VLAN ID.

Port Members

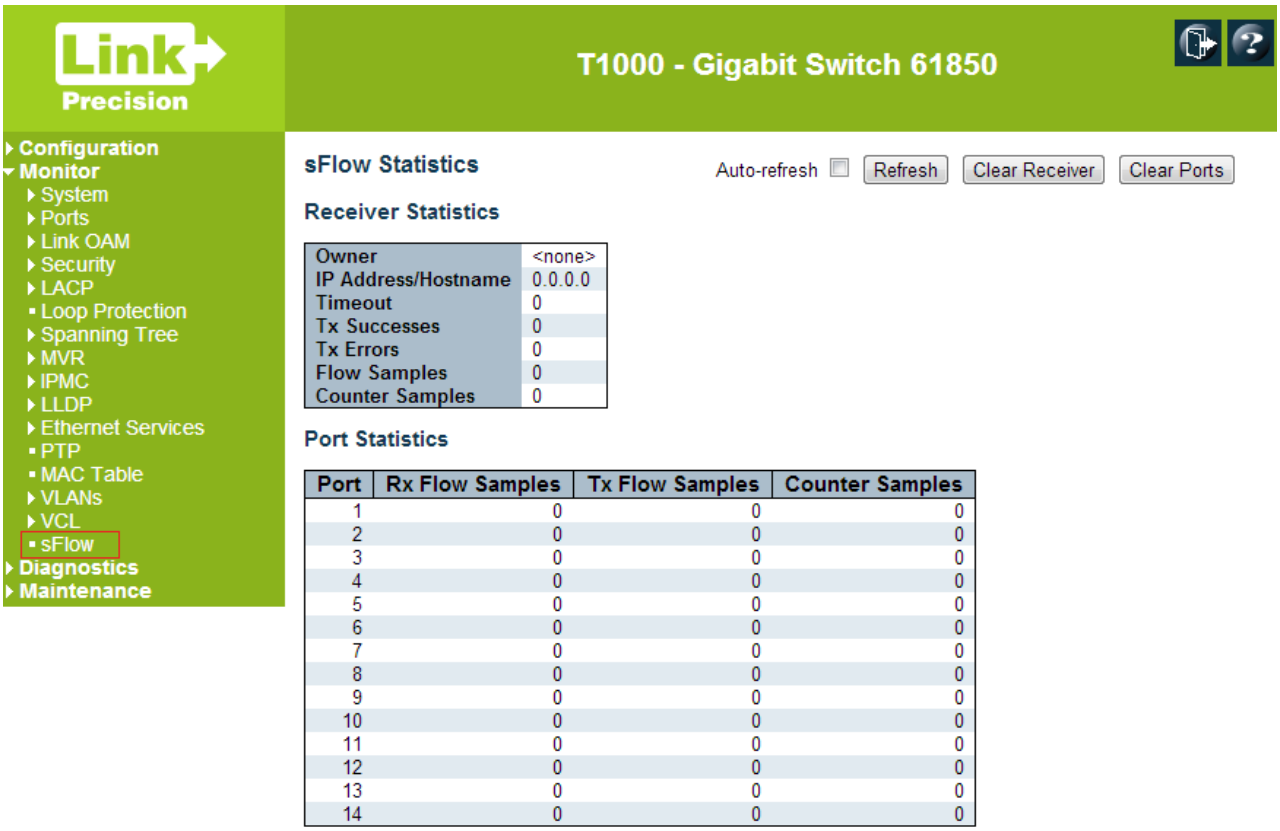
Port members of the MAC-based VLAN entry.

Buttons

AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Refreshes the displayed table.

sFlow

sFlow Statistics



This page shows receiver and per-port sFlow statistics.

Receiver Statistics

Owner

This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:

• If sFlow is currently unconfigured/unclaimed, Owner contains <none>.

• If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.

• If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

IP Address/Hostname

The IP address or hostname of the sFlow receiver.

Timeout

The number of seconds remaining before sampling stops and the current sFlow owner is released.

Tx Successes

The number of UDP datagrams successfully sent to the sFlow receiver.

Tx Errors
The number of UDP datagrams that has failed transmission.
The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics → Ping/Ping6).

Flow Samples
The total number of flow samples sent to the sFlow receiver.

Counter Samples
The total number of counter samples sent to the sFlow receiver.

Port Statistics

Port
The port number for which the following statistics applies.

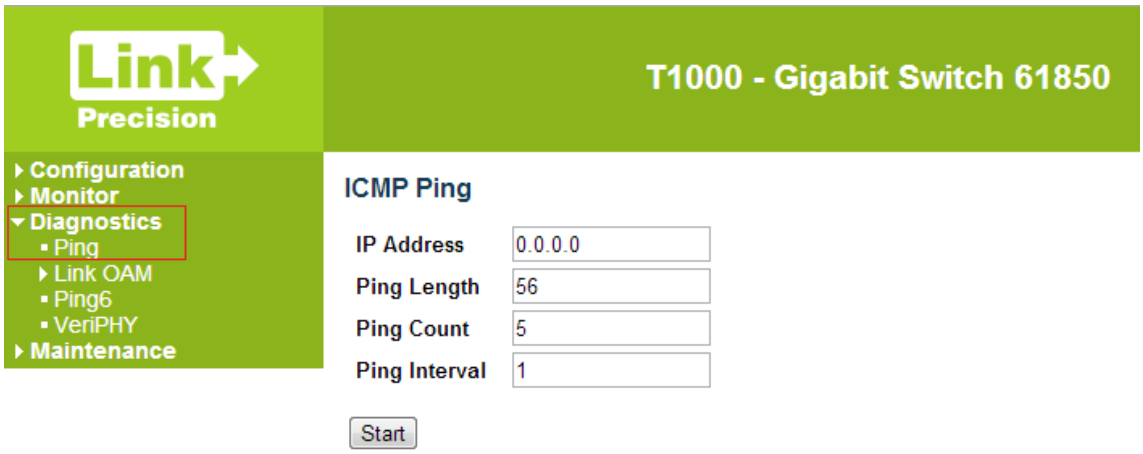
Rx and Tx Flow Samples
The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.

Counter Samples
The total number of counter samples sent to the sFlow receiver originating from this port.

Buttons
AUTO-REFRESH: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
REFRESH: Click to refresh the page.
Clear Receiver: Clears the sFlow receiver counters.
Clear Ports: Clears the per-port counters.

Ping

Ping Configuration



Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.
After you press , ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested data space(the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.
PING server 10.10.132.20, 6 bytes of data.
64 bytes from 10.10.132.20: icmp_seq=0, time=0ms
64 bytes from 10.10.132.20: icmp_seq=1, time=0ms
64 bytes from 10.10.132.20: icmp_seq=2, time=0ms
64 bytes from 10.10.132.20: icmp_seq=3, time=0ms
64 bytes from 10.10.132.20: icmp_seq=4, time=0ms
Sent packets, received OK, 0 bad

Ping6

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.
After you press , ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.
PING6 server ff02::2, 6 bytes of data.
64 bytes from fe80::219:bff:fe2f:b47: icmp_seq=0, time=10ms
64 bytes from fe80::21:8ff:feed:69dd: icmp_seq=0, time=10ms
64 bytes from fe80::219:bff:fe2f:b47: icmp_seq=1, time=0ms
64 bytes from fe80::21:8ff:feed:69dd: icmp_seq=1, time=0ms
64 bytes from fe80::219:bff:fe2f:b47: icmp_seq=2, time=0ms
64 bytes from fe80::21:8ff:feed:69dd: icmp_seq=2, time=0ms
64 bytes from fe80::219:bff:fe2f:b47: icmp_seq=3, time=0ms
64 bytes from fe80::21:8ff:feed:69dd: icmp_seq=3, time=0ms
64 bytes from fe80::219:bff:fe2f:b47: icmp_seq=4, time=0ms

64 bytes from fe80::21:8ff:feed:69dd: icmp_seq=4, time=0ms
Sent packets, received 10 OK, 0 bad
You can configure the following properties of the issued ICMP packets:

IP Address
The destination IP Address.

Ping Length
The payload size of the ICMP packet. Values range from 2bytes to 142 bytes.

Ping Count
The count of the ICMP packet. Values range from 1 time to60 times.

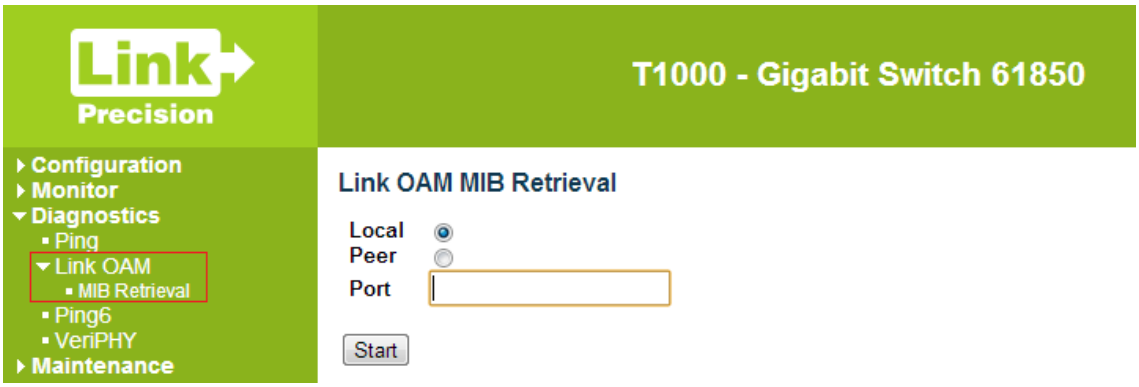
Ping Interval
The interval of the ICMP packet. Values range from 0second to 30 seconds.

Egress Interface (Only for IPv6)
The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes.
The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.
When the egress interfafce is not given, PING6 finds the best match interface for destination.
Do not specify egress interface for loopback address.
Do specify egress interface for link-local or multicast address.

Buttons
START: Click to start transmitting ICMP packets.
NEW PING: Click to re-start diagnostics with PING.

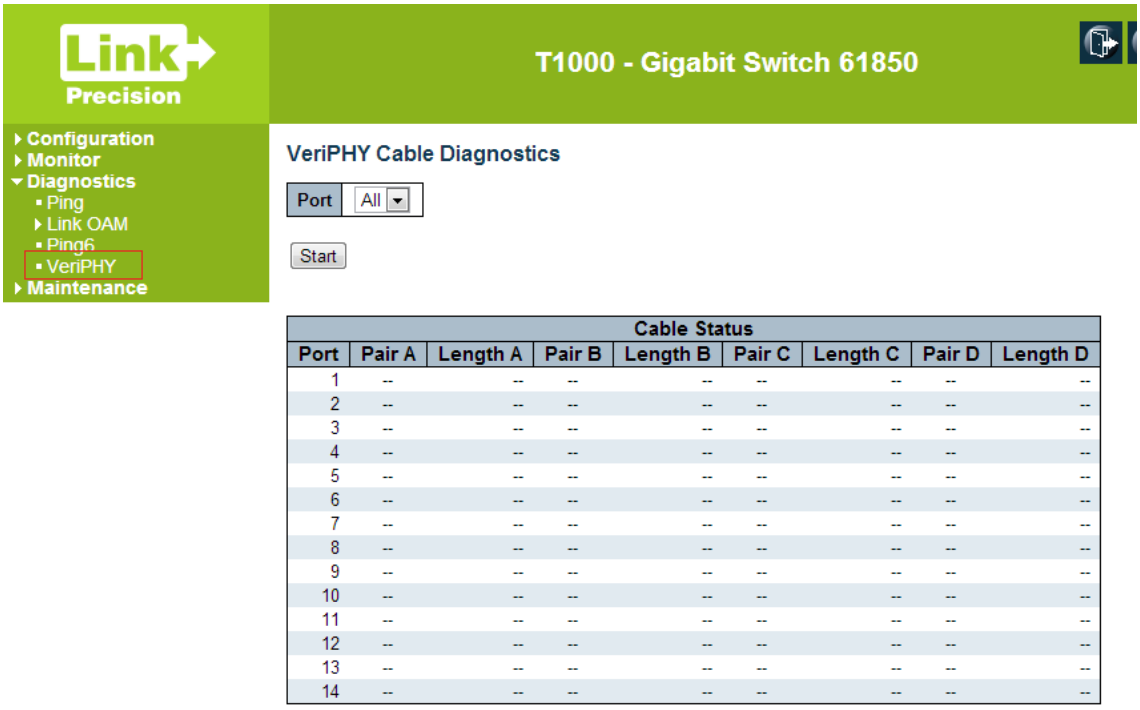
Link OAM

Link OAM MIB Retrieval



This page allows you to retrieve the local or remote OAM MIB variable data on a particular port. Select the appropriate radio button and enter the port number of the switch to retrieve the content of interest. Click on to retrieve the content. Click on to retrieve another content of interest.

VeriPHY


Link
Precision
T1000 - Gigabit Switch 61850
Configuration
Monitor
Diagnostics
Ping
Link OAM
Ping6
VeriPHY
Maintenance
VeriPHY Cable Diagnostics
Port
All
Start
Cable Status
Port Pair A Length A Pair B Length B Pair C Length C Pair D Length D
1 -- -- -- -- -- -- -- --
2 -- -- -- -- -- -- -- --
3 -- -- -- -- -- -- -- --
4 -- -- -- -- -- -- -- --
5 -- -- -- -- -- -- -- --
6 -- -- -- -- -- -- -- --
7 -- -- -- -- -- -- -- --
8 -- -- -- -- -- -- -- --
9 -- -- -- -- -- -- -- --
10 -- -- -- -- -- -- -- --
11 -- -- -- -- -- -- -- --
12 -- -- -- -- -- -- -- --
13 -- -- -- -- -- -- -- --
14 -- -- -- -- -- -- -- --

VeriPHY Diagnostics

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.
Press to run the diagnostics. This will take approximately seconds. If all ports are selected, this can take approximately 1 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.
10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Port

The port where you are requesting VeriPHY Cable Diagnostics.

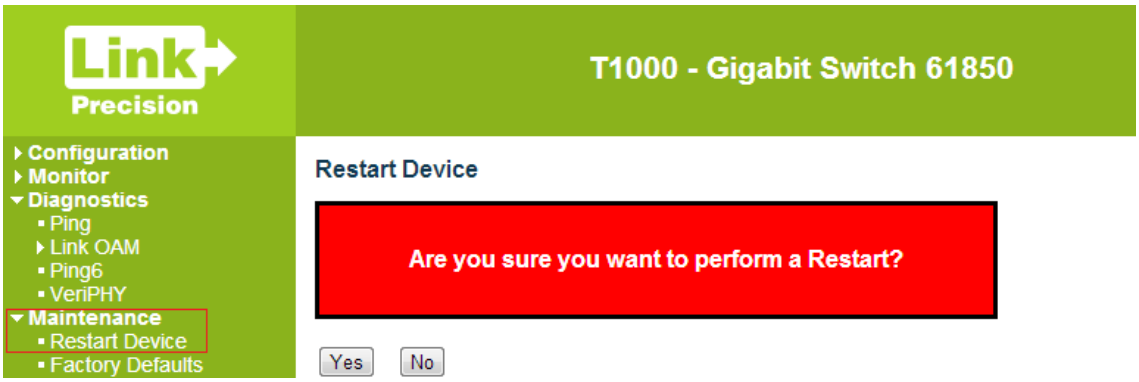
Cable Status

Port:
Port number.
Pair:
The status of the cable pair.
OK - Correctly terminated pair
Open - Open pair

Short - Shorted pair
Short A - Cross-pair short to pair A
Short B - Cross-pair short to pair B
Short C - Cross-pair short to pair C
Short D - Cross-pair short to pair D
Cross A - Abnormal cross-pair coupling with pair A
Cross B - Abnormal cross-pair coupling with pair B
Cross C - Abnormal cross-pair coupling with pair C
Cross D - Abnormal cross-pair coupling with pair D
Length:
The length (in meters) of the cable pair. The resolution is 3 meters

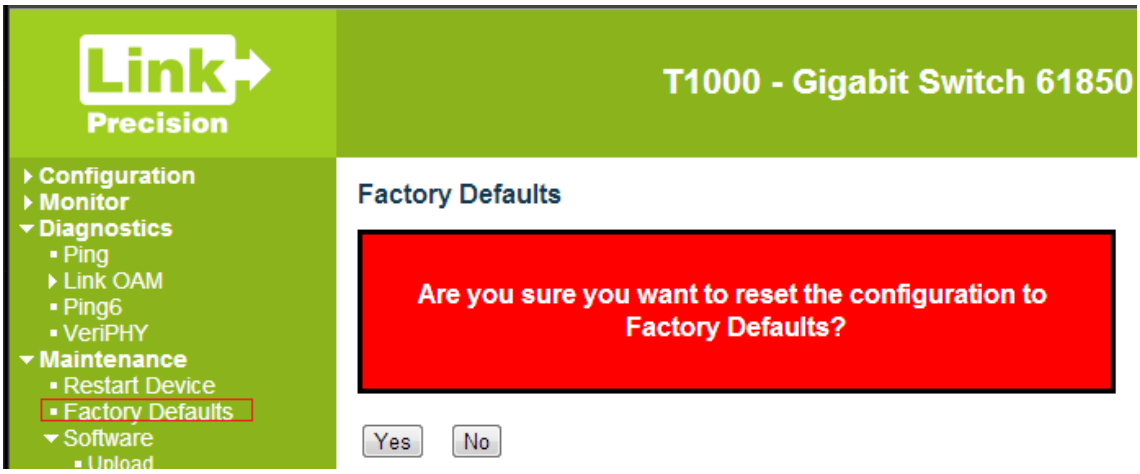
Restart Device

Maintenance Restart



You can restart the switch on this page. After restart, the switchwill boot normally.
Yes: Click to restart device.
No: Click to return to the Port State page without restarting.

Factory Defaults



Maintenance Factory

You can reset the configuration of the switch on this page. Only the IP configuration is retained.
The new configuration is available immediately, which means that no restart is necessary.
Yes: Click to reset the configuration to Factory Defaults.
No: Click to return to the Port State page without resetting the configuration.
Note: Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to default.

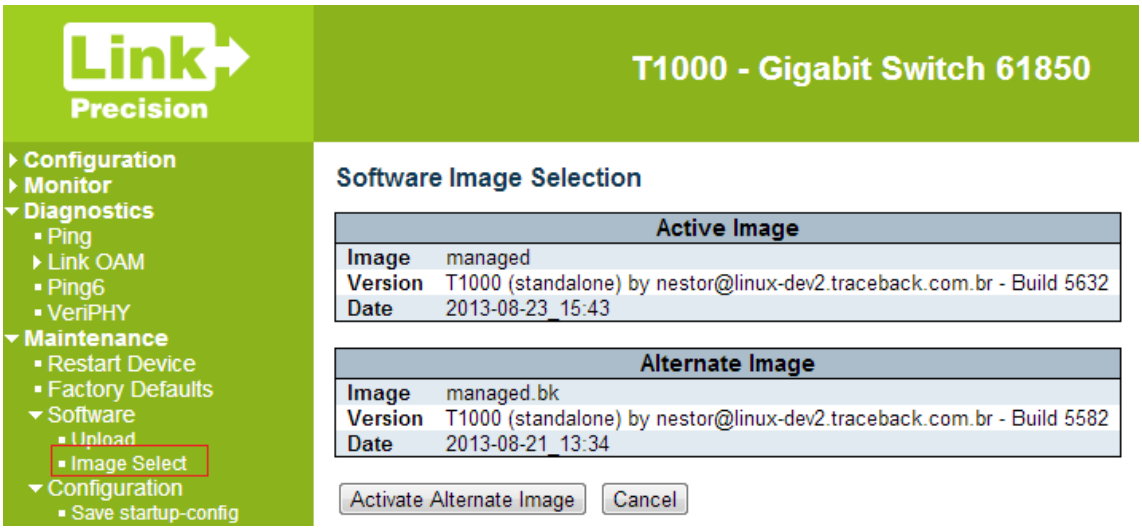
Software

Maintenance Software Upload

This page facilitates an update of the firmware controlling the switch to the location of a software image and click.
After the software image is uploaded, a page announces that the firmware update is initiated. After

about a minute, the firmware is updated and the switch restarts.
Warning: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

Image Selection



This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.
The web page displays two tables with information about the active and alternate firmware images.

Note:
1. In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.
2. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

Image Information

Image
The flash index name of the firmware image. The name of primary (preferred) image is image, the alternate image is named image.bk.

Version
The version of the firmware image.

Date
The date where the firmware was produced.

Buttons
ACTIVATE ALTERNATE IMAGE: Click to use the alternate image. This button may be disabled depending on system state.
CANCEL: Cancel activating the backup image. Navigates away from this page.

Configuration

Running Configuration

Configuration

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.

There are three system files:

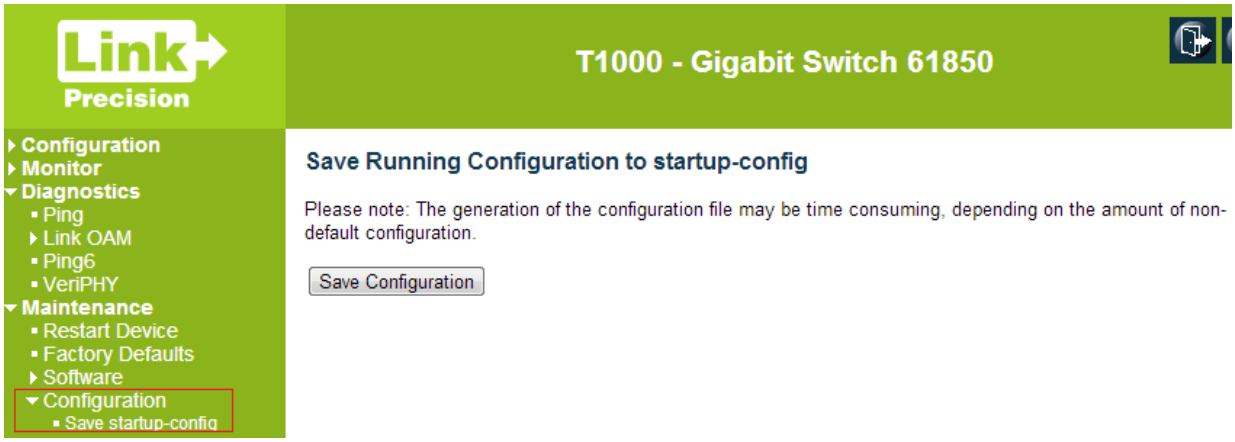
• running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.

• startup-config: The startup configuration for the switch, read at boot time.

• default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

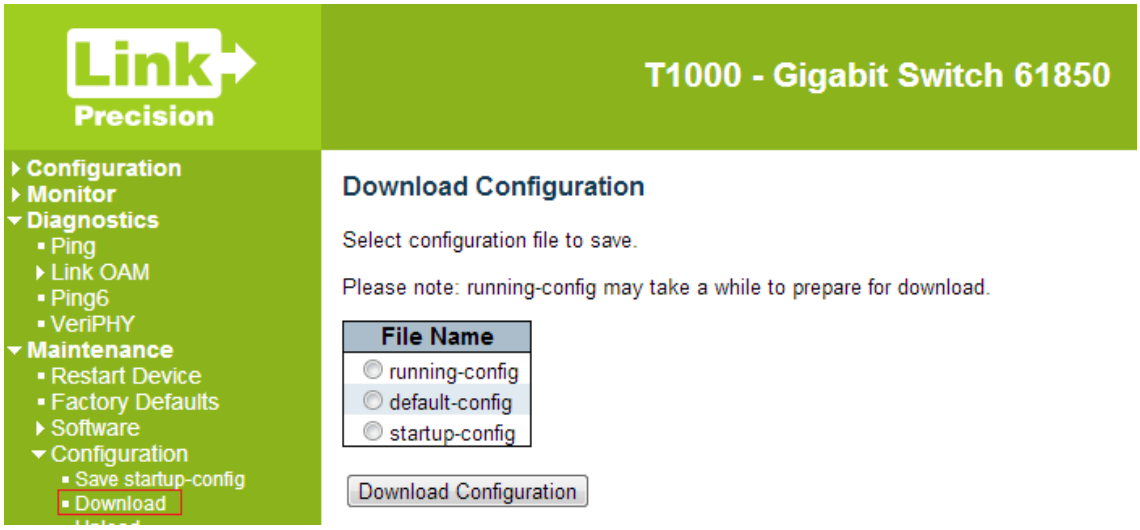
It is also possible to store up to two other files and apply them to running-config, thereby switching configuration.

Save startup-config



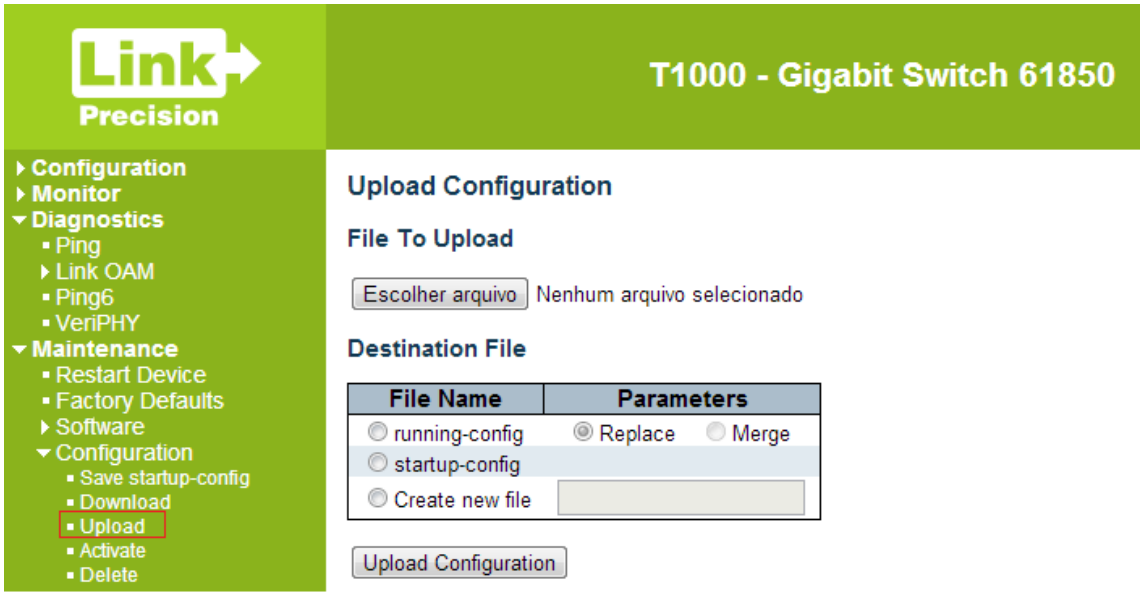
This copies running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.

Download



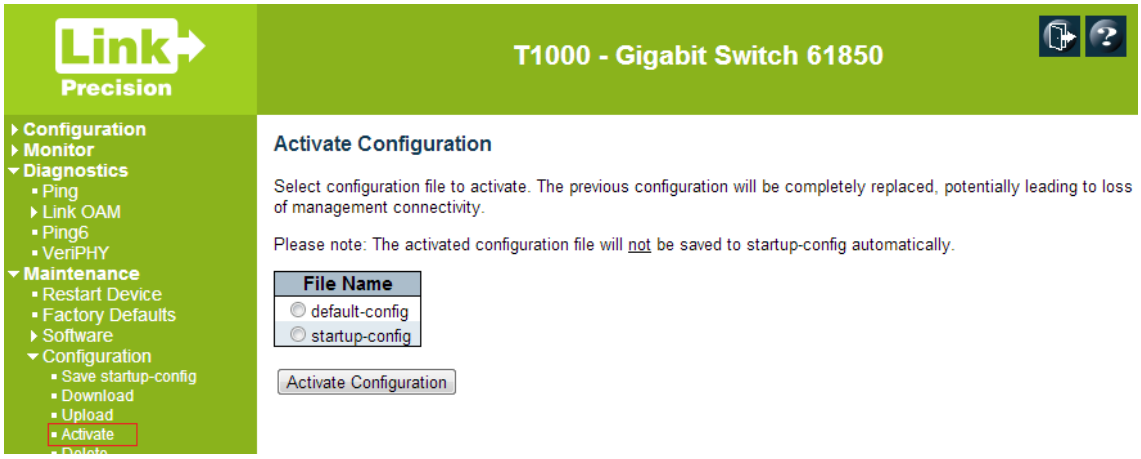
It is possible to download any of the files on the switch to the web browser. Select the file and click . Download of running-config may take a little while to complete, as the file must be prepared for download.

Upload



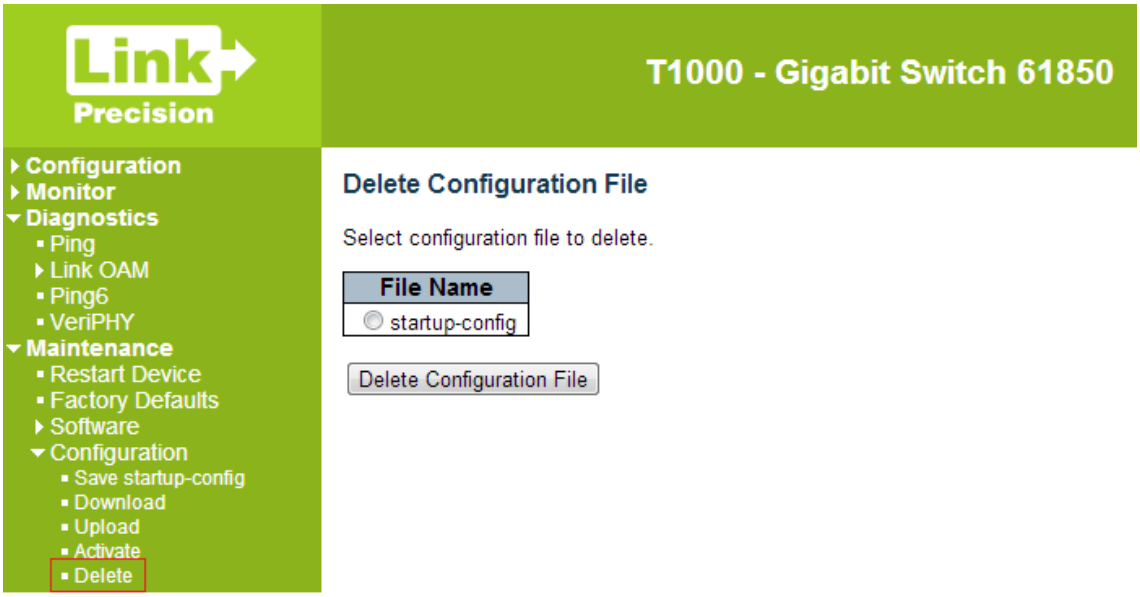
It is possible to upload a file from the web browser to all the files on the switch, except default-config, which is read-only.
Select the file to upload, select the destination file on the target, then click .
If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:
• Replace mode: The current configuration is fully replaced with the configuration in the uploaded file.
• Merge mode: The uploaded file is merged into running-config.
If the file system is full (i.e. contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

Activate



It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.
Select the file to activate and click. This will initiate the process of completely replacing the existing configuration with that of the selected file.

Delete



It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.

Index

AAA, 2, , 4, 46, 48, 64, 213
access, 8, 9, 11, 20, 22, 26, 27, 28, 29, 31, 32, 36, 4, 46, 47, 48, 0, 86, 19, 213, 21, 217, 20, 277
Access Management Configuration, 2, 26
Access Management Statistics, 4, 19
ACL, 2, , 21, 2, 3, 144, 20, 206
ACL Ports Configuration, 2, 2
ACL Status, , 20
activate, 278, 283
Activate, 6, 278, 283
aggregation, 68, 70, 93, 98, 227, 228
Aggregation, 3, 68, 227, 228
Aggregation Static Configuration, 3, 68
ARP Inspection, 2, 21, 9, 61, 62, 63, 211
ARP Inspection Port Configuration, 2, 9
authentication, 23, 28, 29, 32, 33, 36, 4, 46, 47, 48, 49, 0, 6, 66, 199, 200, 204, 21, 216, 261, 263, 26
Authentication Method Configuration, 2, 23
configuration, 8, 1, 22, 23, 42, 43, 4, 46, 47, 48, 49, 0, 3, 7, 9, 61, 80, 8, 89, 92, 97, 103, 108, 109, 110, 112, 114, 122, 14, 146, 148, 10, 14, 16, 19, 160, 161, 162, 168, 170, 171, 172, 190, 196, 197, 198, 213, 21, 27, 263, 264, 266, 267, 276, 279, 280, 282, 283, 284
Configuration, 2, 6, 7, 1, 21, 29, 42, 4, 46, 4, 7, 9, 61, 64, 6, 66, 68, 80, 88, 106, 109, 116, 117, 128, 169, 170, 174, 196, 198, 233, 279
CPU Load, 4, 176
delete, 11, 12, 26, 31, 32, 34, 3, 36, 37, 38, 39, 41, 8, 62, 6, 66, 86, 88, 89, 94, 99, 108, 117, 120, 122, 126, 129, 131, 133, 13, 169, 284
Delete, 6, 11, 12, 26, 31, 32, 34, 3, 36, 37, 38, 39, 41, 8, 62, 6, 66, 86, 88, 89, 94, 99, 108, 110, 112, 114, 117, 120, 122, 126, 129, 131, 133, 13, 169, 284
Detailed Link OAM Port Statistics, 4, 188
Detailed Port Statistics, 4, 186
Detailed System Log Information, 4, 180
DHCP, 2, , 11, 12, 4, , 207, 209
DHCP Relay Configuration, 2,
DHCP Relay Statistics, , 209
DHCP Snooping Configuration, 2, 4
DHCP Snooping Statistics, , 207
diagnostics, 270, 272
Diagnostics, 6, 21, 267, 268, 272
download, 281
Download, 6, 281
DSCP Classification, 4, 14, 18
DSCP Translation, 4, 14, 16
Dynamic ARP Inspection Table, 2, , 63, 211
Dynamic IP Source Guard Table, , 212
Dynamic MAC Table, , 29
ECE Configuration, 4, 142
EPS, 3, 110, 111
EPS Configuration, 3, 110
ERPS, 3, 114, 11
ERPS Configuration, 3, 114
Ethernet Services, 4, , 137, 2
EVC Bandwidth Profile Configuration, 4, 138
EVC Control List Configuration, 4, 140
EVC Port Configuration, 4, 137
EVC Statistics, , 2
factory defaults, 20
Factory Defaults, 6, 276
Group Name to VLAN mapping Table, 4, 133
HTTPS Configuration, 2, 2
IGMP Group Information Table, , 240
IGMP SFM Information Table, , 241, 242, 24, 247
IGMP Snooping, 3, , 92, 94, 96, 238
IGMP Snooping Configuration, 3, 92
IGMP Snooping Port Filtering Profile Configuration, 3, 96
IGMP Snooping Status, , 238
IGMP Snooping VLAN Configuration, 3, 94
Image Selection, 6, 278
information, 10, 48, 49, , 73, 78, 79, 84, 102, 103, 104, 10, 176, 180, 203, 209, 210, 216, 218, 231, 234, 236, 241, 246, 248, 20, 21, 23, 24, 262, 278
IP Configuration, 2, 11
IP Source Guard, 2, 7, 8, 212
IP Source Guard Configuration, 2, 7
IP Status, 4, 177
IPMC, 3, , 86, 87, 88, 90, 92, 96, 101, 238
IPMC Profile, 3, 86, 88, 90, 96, 101
IPMC Profile Address Entry Table, 3, 88
IPMC Profile Configurations, 3, 86
LACP, 3, , 21, 70, 227, 228, 229
LACP Configuration, 3, 70
LACP Port Status, , 228
LACP statistics, , 229
LACP System Status, , 227
levels, 21, 109, 179, 22
Link OAM, 3, 4, 6, 72, 73, 74, 188, 190, 192, 271

Link OAM Link Event Configuration, 3, 74
Link OAM Link Event Status, 4, 192
Link OAM MIB Retrieval, 6, 271
Link OAM Port Configuration, 3, 4, 72, 190
Link OAM Port Configuration Status, 4, 190
LLDP, 3, , 102, 103, 104, 10, 108, 248, 20, 21, 23, 24
LLDP Configuration, 3, 102
LLDP Media, 3, , 10, 20
LLDP Media Configuration, 3, 10
LLDP Neighbour, , 248
LLDP Statistics, , 23
loop protection, 76, 77, 230
Loop Protection, 3, , 76, 230
Loop Protection Configuration, 3, 76
loop protection status, 230
Loop Protection Status, , 230
MAC Address Table Configuration, 3, 116
MAC Table, 3, , 116, 117, 29, 260
maintenance, 20
Maintenance, 6, 21, 112, 274, 27, 276, 277
Maintenance Factory, 6, 276
Maintenance Restart, 6, 27
Maintenance Software Upload, 6, 277
management, 23, 26, 89, 90, 94, 104, 117, 118, 171, 188, 19, 249, 21, 261, 263, 266, 272
MEP, 3, 110, 112, 113, 114
MEP Configuration, 3, 112
method, 23, 39, 48, 49, 202, 224, 20
mirroring, 164
Mirroring, 4, 164
Mirroring Configuration, 4, 164
MLD Group Table, , 24
MLD SFM Information Table, , 246
MLD Snooping, 3, , 89, 97, 99, 101, 243
MLD Snooping Configuration, 3, 97
MLD Snooping Port Filtering Profile Configuration, 3, 101
MLD Snooping Status, , 243
MLD Snooping VLAN Configuration, 3, 99
monitor, 72, 27
Monitor, 4, 49, 0, 73, 83, 173, 262
MVR, 3, , 89, 90, 91, 234, 23, 236, 237, 261, 263
MVR Channels Groups Information Table, , 23
MVR Configurations, 3, 89
MVR SFM Information Table, , 236
MVR Statistics Table, , 234
NAS, 2, 4, , 4, 46, 47, 0, 64, 6, 199, 200, 261, 263, 26
NAS Configuration, 2, 4
NAS Statistics Port, , 200
NAS Switch Status, , 199
network, 11, 12, 4, 47, 48, 8, 72, 83, 84, 8, 89, 94, 9, 99, 102, 10, 108, 109, 13, 140, 164, 177, 220, 222, 223, 249, 20, 21, 22, 261, 263
Network, 2, 4, 12, 42, 10, 108, 141, 142, 177, 196, 20, 21
NTP Configuration, 2, 14
ping, 21
Ping, 6, 267, 269, 270
Ping Configuration, 6, 269
port, 17, 18, 19, 21, 30, 37, 38, 42, 43, 44, 4, 46, 47, 48, 49, 0, 2, 3, 4, , 7, 8, 9, 61, 62, 63, 6, 66, 68, 70, 72, 73, 74, 7, 76, 77, 79, 83, 84, 8, 89, 90, 91, 93, 96, 98, 101, 102, 103, 10, 108, 109, 112, 114, 116, 117, 118, 120, 122, 123, 124, 12, 126, 128, 129, 130, 133, 13, 137, 140, 14, 146, 147, 148, 10, 11, 12, 13, 14, 19, 160, 161, 164, 16, 169, 170, 171, 181, 182, 183, 186, 187, 188, 189, 190, 191, 192, 194, 196, 197, 198, 199, 200, 202, 203, 204, 20, 208, 211, 212, 213, 216, 217, 218, 220, 228, 229, 230, 231, 232, 233, 236, 239, 241, 244, 246, 248, 20, 22, 23, 24, 2, 261, 263, 264, 26, 266, 267, 271, 272, 276
Port Configuration, 2, 18, 43, 47, 76, 103, 164, 171
Port DSCP Configuration, 4, 14
port isolation, 128
Port Isolation Configuration, 3, 128
port security, 43, 196, 197, 198
Port Security, 2, 4, 42, 43, 46, 48, 49, 196, 197, 198, 204
Port Security Limit Control Configuration, 2, 42
Port Security Port Status, 4, 198
Port Security Switch Status, 4, 196
port state, 3, 181, 199, 232
Port State, 4, 0, 181, 199, 200, 27, 276
Port Statistics Traffic Overview, 4, 182
Port to Group mapping Table, 3, 118
ports, 11, 43, 4, 46, 47, 3, 4, 7, 9, 68, 70, 79, 83, 84, 8, 89, 90, 93, 98, 103, 108, 117, 118, 120, 123, 124, 12, 126, 128, 129, 133, 13, 138, 140, 144, 14, 146, 147, 148, 10, 11, 12, 13, 14, 19, 161, 162, 164, 181, 182, 183, 184, 200, 227, 228, 229, 230, 232, 233, 239, 244, 2, 26, 28, 29, 262, 272
Ports, 2, 4, 18, 19, 70, 78, 141, 142, 181, 227, 23, 240, 24, 267
Private VLAN, 3, 126, 127, 128
Private VLAN Membership Configuration, 3, 126
privilege, 20, 21
Privilege Levels Configuration, 2, 21
Protocol to Group Mapping Table, 4, 131
Protocol-Based VLAN, 3, 131
PTP, 4, , 168, 169, 27
PTP Clock Configuration, 4, 168, 169
PTP Clock Monitor, , 27
QCL Status, 4, 184
QoS, 4, 21, 46, 49, 146, 147, 148, 10, 11, 12, 13, 14, 16, 18, 19, 160, 162, 183, 184, 199, 200

QoS Control List Configuration, 4, 19
QoS Egress Port Schedulers, 4, 11
QoS Egress Port Shapers, 4, 12
QoS Egress Port Tag Remarking, 4, 13
QoS Ingress Port Classification, 4, 146, 147
QoS Ingress Port Policing Configuration, 4, 148
QoS Ingress Queue Policing Configuration, 4, 10
QoS Statistics, 4, 183
QoS Weighted Random Early Detection, 4, 162
RADIUS Authentication Overview, , 213
RADIUS Authentication Statistics, , 21
RADIUS Server Configuration, 3, 64
restart device, 27
Restart Device, 6, 27
RMON, 2, , 37, 38, 39, 41, 220, 222, 224, 226
RMON Alarm Configuration, 2, 39
RMON Alarm Overview, , 224
RMON Event Configuration, 2, 41
RMON Event Overview, , 226
RMON History Configuration, 2, 38
RMON History Overview, , 222
RMON Statistics Configuration, 2, 37
RMON Statistics Overview, , 220
running, 132, 174, 200, 213, 214, 216, 218, 272, 279, 280, 281, 282, 283
Running Configuration, 6, 279
Save startup-config, 6, 280
security, 27, 29, 31, 32, 34, 36, 43, 4, 48, , 10, 108, 196, 198, 21
Security, 2, 4, 20, 21, 29, 32, 34, 36, 4, 46, 19, 196, 198
sFlow, 4, 6, 170, 171, 172, 266, 267
sFlow Configuration, 4, 170
sFlow Statistics, 6, 266
SNMP, 2, 26, 27, 28, 29, 30, 31, 32, 43, 171, 261, 263, 26, 266
SNMP System Configuration, 2, 27
SNMP Trap Configuration, 2, 28
SNMPv3 Access Configuration, 2, 36
SNMPv3 Community Configuration, 2, 31
SNMPv3 Group Configuration, 2, 34
SNMPv3 User Configuration, 2, 32
SNMPv3 View Configuration, 2, 3
software, 8, 20, 4, 49, 174, 17, 196, 198, 277
Software, 6, 174, 17, 277
spanning tree, 80, 84, 261, 263
Spanning Tree, 3, , 78, 83, 231, 233, 261, 263
SSH Configuration, 2, 24
Static ARP Inspection Table, 2, 62
Static IP Source Guard Table, 2, 8
storm control, 161
Storm Control Configuration, 4, 161
STP Bridge Configuration, 3, 78
STP Bridge Status, , 231
STP CIST Port Configuration, 3, 83
STP MSTI Configuration, 3, 80
STP MSTI Port Configuration, 3, 8
STP MSTI Priority Configuration, 3, 82
STP Port Statistics, , 233
STP Port Status, , 232
switch, 10, 11, 17, 18, 19, 23, 26, 37, 38, 42, 43, 4, 46, 47, 48, 49, 0, 2, , 64, 66, 68, 70, 72, 73, 74, 77, 78, 82, 83, 8, 89, 90, 93, 98, 102, 103, 114, 117, 118, 120, 122, 124, 126, 131, 133, 146, 148, 10, 11, 12, 13, 14, 161, 162, 166, 171, 174,뒤 17, 179, 180, 181, 182, 183, 184, 186, 188, 192, 19, 196, 199, 200, 201, 202, 20, 21, 217, 227, 228, 229, 230, 231, 232, 233, 239, 244, 21, 23, 24, 271, 272, 27, 276, 277, 279, 281, 282, 283, 284
Switch, 2, , 20, 63, 78, 89, 110, 114, 211, 212, 220, 236, 237, 239, 241, 244, 246, 247, 20, 29
system, 10, 11, 12, 20, 32, 42, 4, 78, 79, 88, 90, 94, 99, 103, 10, 140, 169, 174, 179, 180, 188, 207, 227, 236, 241, 246, 2, 278, 279, 282
System, 2, 4, 8, 10, 11, 17, 21, 42, 4, 2, 86, 103, 106, 174, 179, 227, 228, 248
System access, 2, 8
system information, 10, 174
System Information, 2, 4, 10, 174
System Information Configuration, 2, 10
System Log Configuration, 2, 17
system log information, 179
System Log Information, 4, 179
T1000, 8
TACACS+ Server Configuration, 3, 66
time zone, 1
Time Zone, 2, 1
upload, 20, 282
Upload, 6, 282
UPnP, 4, 166
UPnP Configuration, 4, 166
users, 20, 27, 42, 4, 48, 49, 108, 184, 20, 21, 261, 26
Users Configuration, 2, 20
VCL, 3, 4, 6, 129, 13, 26
VCL IP Subnet-based VLAN Configuration, 4, 13
VCL MAC-Based VLAN Configuration, 3, 129
VCL MAC-Based VLAN Status, 6, 26
VeriPHY, 6, 21, 272
VeriPHY Diagnostics, 6, 272
vlan, , 8, 62, 169
VLAN, 2, 3, , 11, 12, 26, 42, 46, 47, 49, 0, , 8, 9, 61, 62, 63, 80, 89, 90, 91, 94, 9, 99, 100, 108, 109, 112, 117, 118, 120, 122, 123, 124, 12, 126, 128, 129, 130, 132, 133, 13, 136, 140, 142, 143, 144, 14, 146, 147, 19, 169, 198, 199, 200, 203, 204, 211, 212, 234, 23, 236, 238, 240, 241, 243,

24, 246, 21, 22, 29, 260, 261, 262, 263, 264, 26, 270
VLAN Membership Configuration, 3, 122
VLAN Membership Status, , 261
VLAN Mode Configuration, 2, 61
VLAN Port Configuration, 3, 124
VLAN Port Status, , 263
VLAN Translation, 3, 118, 120
VLAN Translation Mapping Table, 3, 120
VLANs, , 49, 0, 61, 80, 89, 94, 99, 108, 122, 123, 12, 126, 130, 136, 199, 200, 261, 263

CORTEC

Variants	Order Number													
	1-	6	7	8	9	10	11	12	13	14	1	16	17-18	19
Model Type														
T1000 IEC 6180 Ethernet Switch	T1000													
Power Supply 1														
110-20 Vdc / 100-240 Vac		3												
Power Supply 2														
110-20 Vdc / 100-240 Vac			3											
Not installed			X											
Mounting options 1														
Ethernet ports on the front				F										
Ethernet ports on the rear				R										
Mounting options 2														
Rack/Panel mounting					P									
DIN rail mounting					D									
Interface Module 1														
Two 1 Gbps RJ4 Cate copper 100BASE-TX/1000BASE-T Ethernet ports						A								
Two slots for up to 1 Gbps SFP transceivers						B								
Two 1 Gbps LC-type connector multi mode fiber 1000BASE-SX Ethernet for up to 0. km						C								
Two 1 Gbps LC-type connector single mode fiber 1000BASE-LX Ethernet for up to 10 km						D								
Two 1 Gbps LC-type connector single mode fiber 1000BASE-ZX Ethernet for up to 40 km						E								

Two 1 Gbps LC-type connector single mode fiber 1000BASE-ZX Ethernet for up to 80 km	F
Two 100 Mbps ST-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km	G
Two 100 Mbps LC-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km	H
Not installed	X

Interface Module 2

Two 1 Gbps RJ4 Cate copper 100BASE-TX/1000BASE-T Ethernet ports	A
Two slots for up to 1 Gbps SFP transceivers	B
Two 1 Gbps LC-type connector multi mode fiber 1000BASE-SX Ethernet for up to 0. km	C
Two 1 Gbps LC-type connector single mode fiber 1000BASE-LX Ethernet for up to 10 km	D
Two 1 Gbps LC-type connector single mode fiber 1000BASE-ZX Ethernet for up to 40 km	E
Two 1 Gbps LC-type connector single mode fiber 1000BASE-ZX Ethernet for up to 80 km	F
Two 100 Mbps ST-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km	G
Two 100 Mbps LC-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km	H
Not installed	X

Interface Module 3

Two 1 Gbps RJ4 Cate copper 100BASE-TX/1000BASE-T Ethernet ports	A
Two slots for up to 1 Gbps SFP transceivers	B
Two 1 Gbps LC-type connector multi mode fiber 1000BASE-SX Ethernet for up to 0. km	C
Two 1 Gbps LC-type connector single mode fiber 1000BASE-LX Ethernet for up to 10 km	D

Two 1 Gbps LC-type connector single mode fiber 1000BASE-ZX Ethernet for up to 40 km	E
Two 1 Gbps LC-type connector single mode fiber 1000BASE-ZX Ethernet for up to 80 km	F
Two 100 Mbps ST-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km	G
Two 100 Mbps LC-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km	H
Two 2. Gbps LC-type connector single mode Ethernet 1000BASE-LX for up to 2 km	R
Not installed	X

Interface Module 4

Two 1 Gbps RJ4 Cate copper 100BASE-TX/1000BASE-T Ethernet ports	A
Two slots for up to 1 Gbps SFP transceivers	B
Two 1 Gbps LC-type connector multi mode fiber 1000BASE-SX Ethernet for up to 0. km	C
Two 1 Gbps LC-type connector single mode fiber 1000BASE-LX Ethernet for up to 10 km	D
Two 1 Gbps LC-type connector single mode fiber 1000BASE-ZX Ethernet for up to 40 km	E
Two 1 Gbps LC-type connector single mode fiber 1000BASE-ZX Ethernet for up to 80 km	F
Two 100 Mbps ST-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km	G
Two 100 Mbps LC-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km	H
Not installed	X

Interface Module

Two 1 Gbps RJ4 Cate copper 100BASE-TX/1000BASE-T Ethernet ports	A
Two slots for up to 1 Gbps SFP transceivers	B

Two 1 Gbps LC-type connector multi mode fiber 1000BASE-SX Ethernet for up to 0. km	C
Two 1 Gbps LC-type connector single mode fiber 1000BASE-LX Ethernet for up to 10 km	D
Two 1 Gbps LC-type connector single mode fiber 1000BASE-ZX Ethernet for up to 40 km	E
Two 1 Gbps LC-type connector single mode fiber 1000BASE-ZX Ethernet for up to 80 km	F
Two 100 Mbps ST-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km	G
Two 100 Mbps LC-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km	H
Not installed	X

Interface Module 6	
Two 1 Gbps RJ4 Cate copper 100BASE-TX/1000BASE-T Ethernet ports	A
Two slots for up to 1 Gbps SFP transceivers	B
Two 1 Gbps LC-type connector multi mode fiber 1000BASE-SX Ethernet for up to 0. km	C
Two 1 Gbps LC-type connector single mode fiber 1000BASE-LX Ethernet for up to 10 km	D
Two 1 Gbps LC-type connector single mode fiber 1000BASE-ZX Ethernet for up to 40 km	E
Two 1 Gbps LC-type connector single mode fiber 1000BASE-ZX Ethernet for up to 80 km	F
Two 100 Mbps ST-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km	G
Two 100 Mbps LC-type connector multi mode fiber 100BASE-FX Ethernet for up to 2 km	H
Not installed	X

PTP Support	
With PTP (IEEE 188) support	P
Without PTP (IEEE 188) support	X
Firmware Version	
Firmware release number	01
Hardware Design Suffix	
Initial release	A

Alstom Grid

© ALSTOM 2014. All rights reserved. Information contained in this document is indicative only. No representation or warranty is given or should be relied on that it is complete or correct or will apply to any particular project. This will depend on the technical and commercial circumstances. It is provided without liability and is subject to change without notice. Reproduction, use or disclosure to third parties, without express written authority, is strictly prohibited.

Alstom Grid Worldwide Contact Centre

www.alstom.com/grid/contactcentre/

Tel: +44 (0) 178 20 070

www.alstom.com